CHAPTER 3

PROPOSED DESIGN OF FACE RECOGNITION SYSTEM

3.1 GENERAL

This chapter describes the design and implementation of face recognition system. Face recognition has received extensive attention in recent years due to its applications in research fields such as biometrics community and computer vision. To identify the optimal algorithm for Multimodal Biometric Authentication System (MMBAS), this chapter discusses various recognition techniques and algorithms for face recognition that are proposed and implemented. They are, content binding of Cryptography with Elastic Bunch Graph Matching (EBGM), Steganography with Bit Plane Complexity Segmentation (BPCS) method, Scale Invariant Feature Transform (SIFT). Factors affecting the result of face recognition and the pre-processing steps that eliminate such abnormalities are also discussed briefly. The objective of this proposed system is to provide insight into different methods available for face recognition, and explore methods that provided an efficient and feasible solution for MMBAS. Single or two biometric traits were used in the above methods and results were compared to identify the optimal approach for the proposed Multimodal Biometric Authentication System (MMBAS) to provide enhanced security.

3.2 NEED AND MOTIVATION

Face recognition is widely considered as one of the most promising biometric techniques, allowing high recognition rates without being too intrusive. Many algorithms were proposed for face recognition and applied in various applications. In the current culture, recognition technology on biometrics, such as palmprint, iris, and face has received much attention (Lin et al. 2005, Xu et al. 2010, Xu et al. 2011, Xu et al. 2012). One of the most delegate biometric technique, face recognition has undergone extensive growth in recent years (Chang et al. 2011). Until now, many methods of face recognition have been proposed. For example, Eigenface (Turk and Pentland 1991), Independent component analysis (ICA) (Zhang
et al. 2007) and Fisher Discriminate Analysis (Wang et al. 2011) are the classic holistic face recognition methods which are simple and effective (Arca et al. 2003). Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Genetic Algorithm (GA), Elastic Bunch Graph Matching (EBGM), Artificial Neural Network (ANN) and Scale Invariant Feature Transform (SIFT) are few other statistical and feature based techniques that are commonly used in solving the face recognition problem.

The research work in face recognition has been carried out in the following directions:

Application domains like online banking, e-voting, online shopping etc. that have not been explored using biometric traits. Proposing a new combination of biometric system, gives very good feature identification accuracy compared to the existing methods. In face recognition, to make changes in existing system Scale Invariant Feature Transform (SIFT) is used to develop local feature extraction. A new combination of dataset using different biometric traits is used in this research.

A face recognition system is expected to identify faces present in images and videos automatically. It can operate in either or both of two modes (Manan Tiwari 2012) namely:

- Face verification (or authentication)
- Face identification (or recognition)

Face verification involves a one-to-one match (ie, 1:1 problem) that compares a query face image against a template face image whose identity is being claimed.

Face identification involves a one-to-many match (ie, 1:N problem) that compares a query face image against all the template images in the database to determine the identity of the query face.

Face is an important research area in biometric authentication system. Iris scanning, for example, is very reliable but too intrusive; fingerprints are socially
accepted, but not applicable to non-consentient people; Palm print is bigger in size. It needs more space to store the image. On the other hand, face recognition represents a good compromise between what’s socially acceptable and what’s reliable, even when operating under controlled conditions. Face recognition provides a lower security level in unconstrained acquisition conditions, but the great advantage of being able to work in places with large concourse of unaware visitors (Daniel Riccio and Gabriele Sabatino 2007). This motivated us to choose face as one of the biometric trait for this proposed method to implement it in various approaches in both UBAS and MMBAS.

3.3 PROPOSED FACE RECOGNITION SYSTEM

Face recognition is a visual pattern recognition problem. Face detection segments the face area from the background. Face recognition, as one of the primary biometric technologies, became more and more important owing to rapid advances in technologies such as digital cameras, internet and mobile devices, and increased demands on security. Face recognition has several advantages over other biometric technologies: It is natural, nonintrusive, and easy to use.

The proposed research is carried out in the following manner using unimodal and multimodal biometric trait to identify the best approach for Multimodal Biometric Authentication System (MMBAS).

- Face detection system with a combination of Cryptographic techniques Message Digest (MD5) and Secure Hash Algorithm (SHA1) with Elastic Bunch Graph Matching (EBGM) algorithm
- Face recognition using Scale Invariant Feature Transform (SIFT)
- A combination of face and finger print authentication system using Bit Plane Complexity Segmentation (BPCS) method with steganography

Many recent researches show that local features are more effective to describe the detailed and stable information of an image. Applications are in the real time environment to implement the recognition system, like E-trading, online
banking, E-voting or internet voting etc. But among these, the online remote voter registration systems face some critical security problems (Election Law Blog 2007). These problems are mainly related to the inability to accurately verify the identity of the voter, which can facilitate impersonation or multiple registrations by the same voter with different data. The proposed system takes this issue as an application domain and it introduces a remote voter registration scheme, in which biometric systems play an important role to protect the accuracy of the electoral roll (Victor Morales et al. 2008 and Mohammed Khasawneh and Mohammad Malkawi 2008). Biometric systems have been already considered in electronic voting in the voting phase.

In this system the first step consists of checking by registration officers where they have to see whether the voter included in the form is the same that is stored in the voter register. Some examples could be the date of birth, the social security number or any other familiar information (e.g., mothers’ maiden name, etc.). The problem with using such information for identifying the voter is that this information could be available in other databases (e.g., the member database of a social club) or could be known by people close to the voter. The second step consists of verifying the identity of the voter based on checking some voter personal characteristics, such as a handwritten signature stamped on the form or the face or fingerprint of the voter against an image or template contained in some identity card or database.

3.3.1 Issues in current online remote voting systems

The existing online remote voter registration methods do not check whether the same person has filled more than one registration form by using the names of different valid voters. The contents of the registration form can be altered after the voter has sent this form. The problem identified in handwritten signature is that, it is not bound to the contents of the register. Therefore, the current voter registration systems face the following problems (Victor Morales et al. 2008):

- Accuracy to the voter identity validation
➢ Prevention of multiple registration by voters

➢ Integrity of voter registration information on modification

To overcome the above problems the proposed method is implemented in e-voting application. The main idea of proposed method is to bind the contents of the registration form to the identification element (i.e. the biometric characteristic). It evaluates how to take advantage from the most usable biometrics to carry out the voter registration process in a more effective way. To increase the accuracy of remote registration process, the proposed method combines the multiple biometric traits in MMBAS. The following section describes about the various experiments which are carried out in face recognition system.

3.4 EXPERIMENTS

This experimental section discusses the implementation process of various algorithms and comparison of the algorithms to identify the optimal system which suits for Multimodal Biometric Authentication System (MMBAS). Subsection 3.4.1 describes the implementation of combining cryptographic (MD5 & SHA1) techniques with Elastic Bunch Graph Matching (EBGM) algorithm for hash key generation to identify the face. Subsection 3.4.2 discusses about the implementation of face recognition using Scale Invariant Feature Transform (SIFT). Subsection of 3.4.3 explains about implementation of face and fingerprint detection using steganography with Bit Plane Complexity Segmentation (BPCS) algorithm. The proposed scheme of voting process is divided in two main stages:

➢ Introduction of the voter registration information and protection of the integrity

➢ Generation and validation of a registration proof

The validation process facilitates the detection of people who attempt to create more than one record. It is possible to compare the face of a voter who is validating a new registration with the set of faces previously recorded in the database. That way, a person attempting to create a bogus or an additional record
will be rejected, and the registration information associated with the proof provided by such a person will be identified as invalid. Therefore, the probability of impersonation is low. This verification is not necessarily carried out on-line but it can be made after the registration process.

From the above three implementation processes it can be identified that, the algorithm which provides optimal solution can be considered and implemented in Multimodal Biometric Authentication System (MMBAS) to provide highest level of security to the information.

3.4.1 Implementation of Cryptographic Algorithms

Implementing cryptographic algorithm in proposed approach in this section is as follows:

- Generating Hash key by means of creating the integrity proof using the combination of MD5 and SHA1 hash functions
- A face biometric trait is used for the generation of a registration proof and the validation of the registration information
- For face recognition, feature based Elastic Bunch Graph Matching (EBGM) algorithm is used to recognize unique faces by first localizing a set of landmark features, approximation of landmark features, and then measuring similarity between these features

The proposed work discusses about the combination of face biometric trait with cryptographic hash function. This proposal carries out a remote voter registration in a secure way. It protects from alterations the contents of the voter registration information by binding such information to the voter identity. This is reached by means of combining biometrics and cryptographic (content binding) techniques that do not require a public key infrastructure. Cryptology is an important tool in the area of information security. Cryptology can provide data secrecy, integrity, usability and non-repudiation. Cryptology mainly consists of two parts, cryptography and cryptanalysis. The top task of cryptography is to hide data using
coding technology, while cryptanalysis is about obtaining the plaintext from cipher text (Shen Changxiang et al. 2007). Hence, cryptographic algorithms can be divided into three classes in modern cryptology namely Public key algorithms, Symmetric key algorithms, and Hash functions.

While the first two are used to encrypt and decrypt data, the hash functions are one-way functions that do not allow the processed data to be retrieved. This work focuses on hashing algorithms. Currently, the most commonly used hash functions are the MD5 (Klima 2005) and the Secure Hash Algorithm (SHA), with 128- to 512-bit output Digest Messages (DMs), respectively. SHA-1 was approved by the National Institute of Standards and Technology (NIST) in 1995 as an improvement to the SHA-0. SHA-1 quickly finds its way into all major security applications, such as SSH, PGP, and IPSec (Veerla Hema Hanumakumar et al. 2011).

Cryptographic hash functions use a string of any length as its input, and output one with constant length. Here, assume $y = h(x)$, where $h$ is a hash function, which has to meet the following requirements:

$$y = h(x); \quad (3.1)$$

- The length of $x$ is arbitrary, while the length of $y$ is constant
- For a given $x$, it is easy to compute $y$, while, for a given hash value $y$, it is hard to find $x$ to satisfy
- It is computationally unfeasible to find two different inputs $x$ and $x'$ and

$$h(x) = h(x'); \quad (3.2)$$

The significant purpose of hash functions is to provide the verification of data integration and validity. Today, there are numerous constructions for hash functions, including three categories:
Based on several mathematical hard problems, such as integer factoring, discrete logarithm problems

Based on some symmetry cryptology systems, such as DES design

Not based on any assumptions, whereas using directly cryptographic construction instead (McLoone and McCanny 2002). These categories of Hash functions cover some famous ones, for example, SHA-1, SHA-256, SHA-384, SHA-512, MD4, MD5, RIPEMD, HAVAL.

There are two main operation contexts implemented by biometric systems for user authentication in the existing systems (Sonja Hof 2004):

- Current remote hand-writing signature uses the verification context method only (Kalera et al. 2004)

- Using voice biometric system in the identification context, the signature of the register could be checked against the complete database of signatures stored

But in the above cases the same voter attempts to register more than once using different login and it is ease to do the fraudulent activity (Alexander Prosser et al. 2008).

In this process, four participants are necessary during the voter registration process: a citizen requesting to be a voter, a registration module, a validation module and the registration officer (Victor Morales et al. 2008).

- Voter - The voter provides her personal data in order to generate the registration information. The voter also will collaborate to generate a registration proof based on both, her biometric characteristic and the registration information.

- Registration module - This module is used to enter the voter registration information and generate an integrity proof of such registration information
- Validation module - The registration proof is generated by means of this module. Such proof is generated with the biometric information provided by the voter.

- Registration officers - The registration officers receive the voter register information and carry out some validation processes.

Based on this division the scheme behaves as follows.

The voter carries out a communication with the validation module. This communication is done by means of web camera. Then the voter is asked to give the integrity proof. He or she types the proof previously shown by the registration module, i.e. the groups of characters that represent the integrity proof. Current remote voter registration systems have important issues that can facilitate voter impersonation.

Message Digest Algorithm (MD5) is used to verify data integrity. It creates a 128-bit message digest from data input (which may be a message of any length) that is claimed to be unique (Wang 2005). If as little as a single bit value in the file is modified, the MD5 value for the file will completely change. Forgery of a file will be extremely difficult. Secure Hashing Algorithm (SHA1) is used to provide authenticity. SHA1 is the original 160-bit hash function. SHA-1 is most widely used among the existing SHA hash functions, and is employed in several widely-used security applications and protocols (Veerla Hema Hanumakumar et al. 2011).

The integrity proof is generated using the combination of MD5 and SHA1 hash functions. The latest is used in its Message Authentication Code (MAC) implementation. Message Authentication Code (MAC) is another protection scheme proposed first in 1970s that aims to enforce lattice-based information flow constraints to create high-assurance information systems with confidentiality, integrity, and aggregation concerns. In practice, convert channel remains a major impediment for implementing MAC. This combination is conceived with the aim of preventing collision between the digest messages (Wang 2005).
Message Authentication Code (MAC) is designed especially for applications where data integrity is required. MAC involves cryptographic processing in which both communicating parties share a symmetric secret key K which is not known to anyone else. Sender calculates the MAC by first calculating message digest of the message or document and then applying secret key K to the message digest. Sender then sends original message or document along with calculated MAC to the receiver (Harshvardhan Tiwari and Krishna Asawa 2010). Receiver independently computes a MAC over the message and compares the computed MAC to the received MAC. If it matches then receiver conclude that message has not been altered during transit and if does not match then rejects the message, realizing that the message was changed during transit. Figure 3.1 shows generating identity proof using MD5 and SHA1 algorithm for voter’s information.

The generation of integrity proof is as follows:

- Get a digest \( K \) from the registration information
  
  \[ M_i: K = \text{MD5}[M_i] \quad (3.3) \]

- Use \( K \) as a key to get a HMAC--SHA1 from the same registration information
\( M_i \cdot H = \text{HMAC-SHA1} [M_i, KM_i, K] \)  \hspace{1cm} (3.4)

The resultant \( H \) is the integrity proof. Using a combination of MD5 and HMAC-SHA1, the probability to have a collision decreases significantly. An attacker needs to find a coincidence of collision for the same text on both systems. In addition, proposed method reduces the probability of these collisions without increasing the size of the digest that remains the same as a SHA1 (160 bits). Since \( H \) is based on an HMACSHA1, it is 160 bits long, i.e. 2^{160} different digests. Therefore, a base-32 notation allows a representation of SHA1 in 32 characters. These 32 characters can be shown to the voter in six groups of five characters plus the two remaining ones (Victor Morales et al. 2008). However, the integrity proof \( H \) can be truncated in order to give a higher usability. For example, taking only the first 20 characters, they can be shown in five groups of four characters, which is usable enough.

The issues in e-voting process are voter identification accuracy, multiple registrations from the same person and voter registration information integrity. From the proposed system it has been proved that, the use of biometric systems will increase the voter identification accuracy of voters that make a remote registration. Current remote voter registration systems have important issues that can facilitate voter impersonation.

### 3.4.1.1 Biometric System Design

The voter registration systems may use biometrics system. Registration module verifies physical characteristics that uniquely identify the voter. The proposed biometric system is used to help registration officers to improve the accuracy of voter identification. Biometric systems are electronic systems specialized on identifying a user by means of processing unique physiological or behavioural characteristic of the user. Elastic bunch graph matching (EBGM) technique is one of the promising techniques in the field of biometric. Also it found better results with EBGM method than other existing methods like Artificial Neural Networks (ANN), PCA, ICA, Gabor jets, Linear Discriminant Analysis (LDA or Fisher-faces), and Hybrid methods. It is recommended that a hybrid technique
involving EBGM algorithm may be used to obtain better results. The system which is implemented using Elastic Bunch Graph Matching (EBGM) algorithm for face recognition process will fulfil all the biometric requirements (Laurenz Wiskott et al. 1999). The Figure 3.2 shows the model graphs of Elastic Bunch Graph Matching (EBGM) algorithm.

![Figure 3.2 Model graph for varying faces using EBGM algorithm](image)

Face recognition is a complex and difficult process due to various factors such as variability of illumination, occlusion, face specific characteristics like hair, glasses, beard, etc., and other similar problems affecting computer vision. Using a system that offers robust and consistent results for face recognition, various applications such as identification for law enforcement, secure system access, computer human interaction, etc., can be automated successfully. Face recognition using elastic bunch graph matching is based on recognizing unique faces by estimating a set of distinct features using a data structure called a bunch graph. Similarly for each query image, the landmarks are estimated and located using bunch graph (Laurenz Wiskott et al. 1999). Then the features are extracted by convolution with the number of instances of Gabor filters followed by the creation of face graph. The matching score is calculated on the basis of similarity between face graphs of database and query image.

The algorithm recognizes novel faces by first localizing a set of landmark features and then measuring similarity between these features. The EBGM algorithm is easily divided into three steps. The first step is to determine the Landmark locations. Next, a face graph is created for every image that needs to be matched. The similarity of face graphs is computed and final classification is based on this similarity (Jagmeet Singh Brar and Sonika Jindal 2012). But in the proposed method
only particular fiducial points are selected. The proposed method is implemented based on capturing the image of the voter, loading the face image of the voter in the system, reading and resizing the image, and obtaining RGB, height and width of the image to detect the face of the voter. The modules involved in face recognition process are data acquisition, fiducial point extraction and storage, pre-processing, and face matching.

Figure 3.3 shows the proposed face detection modules in cryptographic approach. In phase I the system loads and reads the image, and then it extracts the skin and removes the noise.

![Figure 3.3 Illustration of proposed face detection modules in cryptographic approach](image)

In phase II the extracted image finds the fiducial point extraction and match with the reference template. The proposed approach takes into account the human facial features and is totally different to Eigen face and Fisher face (Sushma Jaiswal et al. 2010). It uses elastic bunch graph to automatically locate the fiducial points on the face (eyes, nose, mouth etc) and recognize the face according to these face features. The proposed algorithm uses the structure information of a face which
reflects the fact that the images of the same subject tend to translate, scale, rotate, and deform in the image plane. It makes use of the labelled graph in which, edges are labelled with the distance information and nodes are labelled with wavelet coefficients in jets. This model graph can then be used to generate image graph. The model graph can be translated, scaled, rotated and deformed during the matching process.

### 3.4.1.2 Results

This section describes about the results of comparison with the existing system. By using EBGM algorithm the voter face can be detected based on various factors. After implementing the EBGM algorithm in face recognition process, the approved voter face is detected. The representation of local features is based on Gabor wavelet transform. Gabor wavelets are biologically motivated convolution kernels in the shape of plane waves restricted by a Gaussian envelope function. The set of convolution coefficients for kernels of orientations and frequencies at one image pixel is called a jet.

The graph is positioned over the input image. At each node, the local jet around the corresponding image point is computed and stored. This pattern of jets is used to represent the pattern classes. A new image is recognized by transforming it into a grid of jets and comparing it to known models. In EBGM each node is a set of jets, each derived from a different face image. Pose variation is handled by...
determining the pose of the face using prior class information. The jet transformations under variations in pose are then learned.

A jet describes a small patch of grey values in an image \( I(\bar{x}) \) around a given pixel \( \bar{x} = (x, y) \). It is based on a wavelet transform defined as a convolution,

\[
J(\bar{x}) = \int I(\bar{x}') \psi_j(\bar{x} - \bar{x}') \, d^2 \bar{x}'
\]

The proposed method determines the binary pattern of face fiducial point extraction based on the following process.

Step 1: Jets are selected by hand to serve as examples of facial features.

Step 2: A bunch graph is created. Each node of the bunch graph corresponds to a facial landmark and contains a bunch of model jets extracted from the model images.
Figure 3.6 Bunch graph creation corresponds to facial landmark

Step 3: Landmark points are located for every image. First, a novel jet is extracted from the novel image. The novel jet’s displacement from the actual location is estimated by comparing it to the most similar model jet from the corresponding bunch.

Step 4: A face graph is created for each image by extracting a jet for each landmark. The graph contains the locations of the landmarks and the value of the jets. The original image can then be discarded.

Step 5: Face similarity is computed as a function of landmark locations and jet values.

The unique jet points with estimated displacement of actual landmark and the possible face with detected fiducial point extraction is shown in Figure 3.7 and Figure 3.8 respectively.

Figure 3.7 Illustration of unique jet points with estimated displacement of actual landmark
In some way, the voter registration systems previously described are based on the use of biometrics. Registration officers usually verify some physical characteristics that uniquely identify the voter, such as an image (facial identification) of the voter. However, one of the main issues of this identification is the accuracy on the process, since not all the registration officers are, for example, handwriting or physiological experts. In this sense, the proposed system uses the biometric systems to help registration officers to improve the accuracy of voter identification. However, the accuracy on the different biometric system is not the same, since each of the biometric characteristic being processed has its advantages and disadvantages.

The proposed method is compared with other existing biometric systems based on the biometric characteristics and that is shown in Table 4.1. A good biometric characteristic must fulfil some requirements (Prabhakar et al. 2004):

- **Universality** - Each individual should have the characteristic
- **Uniqueness** - How well the characteristic makes different between two individuals
- **Permanence** - How well the characteristic endures over time
- **Collectability** - Ease of acquiring the characteristic
Performance - Refers to the speed and accuracy of recognition as well as the resources required to do it (cost)

Acceptability - It indicates the level of acceptance of people to use the characteristic

Robustness - It reflects the level of resistance against fraudulent methods attempting to mislead the system

Table 3.1 Comparison results of various biometric traits based on Quality attributes

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Universality</th>
<th>Uniqueness</th>
<th>Permanence</th>
<th>Collectability</th>
<th>Performance</th>
<th>Acceptability</th>
<th>Robustness</th>
<th>Content Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint (Uludag 2004)</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>---</td>
</tr>
<tr>
<td>Signature Off-line (Kalera et al. 2004)</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>NO</td>
</tr>
<tr>
<td>Face (Proposed System)</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>YES</td>
</tr>
</tbody>
</table>

It was identified that the existing fingerprint and signature biometrics were not able to do the content binding. Table 3.1 shows the comparison of existing biometrics with the proposed biometric characteristics which is used as Unimodal Biometric Authentication system (UBAS). The proposed biometric systems fulfil the requirements previously introduced in a three point scale of L=Low, M=Medium and H=High.
Based on the operation of both contexts, the proposed system can identify that current remote voter registration methods only use the verification context; registration officers use voter personal information to retrieve the image stored in their database for comparison. However, using a biometric system in the identification context, the image of the register could be checked against the complete database of images stored. Then, in case the same voter attempts to register more than once using different personal information, he/she will be detected. Therefore, the use of an identification context prevents multiple registrations by voter.

From this comparison it can be concluded that off-line signatures and voice biometrics are not as robust as fingerprint biometric systems. However, the introduction of face biometrics could improve the current systems. Another important aspect of performance on biometrics is the accuracy of the identification process. There are three parameters that can help to determine the accuracy in a quantitative manner.

- **False Rejection Rate (FRR).** It is the percentage of eligible user requesting access declared by the system as non-eligible;

- **False Acceptance Rate (FAR).** It is the percentage of non-eligible access attempts identified as valid users;

- **Equal Error Rate (EER).** The point at which FRR and FAR are the same

Additional comparative analysis of the same biometrics systems used in Table 3.2, provide the following measures from the accuracy point of view.
Table 3.2 Performance based comparison results of the biometric systems

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>FRR (in %)</th>
<th>FAR (in %)</th>
<th>EER (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint (Uludag et al. 2004)</td>
<td>2.2</td>
<td>2.2</td>
<td>2.2</td>
</tr>
<tr>
<td>Signature Off-line (Kalera et al. 2004)</td>
<td>10-30</td>
<td>10-30</td>
<td>10-30</td>
</tr>
<tr>
<td>Voice (Przybocki and Martin 2004) and</td>
<td>5-10</td>
<td>2-5</td>
<td>6</td>
</tr>
<tr>
<td>Reynolds 2004)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Face (Proposed method)</td>
<td>10</td>
<td>2</td>
<td>3.5</td>
</tr>
</tbody>
</table>

Based on the values shown in Table 3.2, it can be inferred that fingerprints and face are the best biometric characteristic. From the proposed work face biometrics can also bind the registration information to the voter identity. Combining this feature with the use of cryptographic algorithms, such as hash functions, it provides a way to protect the integrity of voter registration information that can be suitable to implement in current environment. The proposed method will protect from alterations the contents of the voter registration information by binding such information to the voter identity. The error rates of biometric system and the point at which FRR and FAR is equal. A lower EER value which indicates better performance of the proposed method can increase the recognition to overcome the enrolment problem and enhance the security.

The identity proof is verified with the voter details and the voter is allowed to give their personal characteristics to poll their vote. By doing this process, the face of the voter is bound to the contents of the registration information. The registration proof is then stored by the validation module. The validation process facilitates the detection of people who attempt to create more than one record. Therefore, the probability of impersonation is low in this proposed system. If a biometric is used for access device, a false reject may be acceptable, as it may only
require the user to use a different means of authentication. In the context of e-voting, a false reject means to deny an individual of the possibility to execute his/her right as a citizen. From the proposed method it is proven that the e-voting process is easy to access and it provides the highest level of security.

3.4.1.3 Discussion of Results

In the past few years various cryptanalysis results have shown that a variety of cryptographic hash functions based on design principle of MD4 are vulnerable to the collision attack. Among these hash functions MD5 and SHA-1 are widely deployed in various cryptographic applications. Although flaws have been found in these algorithms they are still in use today (Harshvardhan Tiwari and Krishna Asawa 2010). This may pose a serious security problem. MD-5 and SHA-1 should be replaced and should not be used further for applications. MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures. Any user who can verify a MAC is also capable of generating MACs for other messages. MAC also faces key exchange problem. As a result, MAC-based schemes have found limited applicability in highly legislated environments such as military. MACs rigidity makes it difficult to adapt it for a social network context.

The Elastic Bunch Graph Matching (EBGM) algorithm is one of the promising techniques in face recognition (Sachin Katadound 2004). Also it gives better results with EBGM than PCA in the current trend. But, EBGM method takes a long time to train and generate distance measures for the given gallery images compared to PCA. As far as the drawback of EBGM algorithm is concerned, it is very sensitive to lightening conditions and that a lot of graphs have to be placed manually on the face. A reliable system needs recognition then it is compared with graphs, but it requires huge storage of convolution images for better performance.
The above method is suitable for Unimodal Biometric Authentication System (UBAS), but many complexities as mentioned above have to be faced if this method is applied on biometric traits. So, to overcome these limitations, the research focuses on Scale Invariant Feature Transform (SIFT) algorithm on face recognition system to improve the data security, accuracy, and to reduce the cost of the system.

### 3.4.1.4 Dataset and System Requirement

This face database comprises 50 images from 25 persons. There are 15 females and 10 males, each of whom has two images (xa and xb) with different facial expressions. The xa images are used as gallery for training while the xb images as probes for testing. All the images are randomly selected from the local face database.

This part of the proposed method is implemented in Microsoft.Net Framework 2.0 Integrated Development Environment using ASP.Net. This enables the system to be installed and executed on any computer platform. The data tables at the backend in the servers are all developed using SQL Server 2005. It has a Pentium(R) Dual-Core CPU@2.60GHz, and 4G memory, running Windows 7.

### 3.4.2 Face recognition using Scale Invariant Feature Transform (SIFT)

Face recognition is non-intrusive, has high user acceptance, and provides acceptable levels of recognition performance in controlled environments, robust face recognition in non-ideal situations continues to pose challenges (Anil K. Jain and Ajay Kumar, 2010). Face recognition systems typically utilize the spatial relationship among the locations of local facial features such as eyes, nose, lips, chin, and the global appearance of a face. Many different approaches to recognition as a correspondence of local features have been proposed in literature (Gyuri Dork’o and Cordelia Schmid (2003), Krystian Mikolajczyk and Cordelia Schmid (2005), David G. Lowe (1999), Frederik Schaffalitzky and Andrew Zisserman (2001), Frederik Schaffalitzky and Andrew Zisserman (1999)), and with them many different descriptors. One well known descriptor is the Scale Invariant Feature Descriptor (SIFT) developed by David G. Lowe in 1999. It detects points of interest
with invariance to scale, rotate and translate. Schmid and Mikolajczyk have evaluated the performance of five different interest point descriptors (Krystian Mikolajczyk and Cordelia Schmid 2005). The criterions used were that the descriptors should be distinctive and at the same time robust to changes in viewing conditions as well as to errors of the point detector. The result of the evaluation was that the SIFT descriptor performs best. A great advantage of Lowe’s object recognition system is that it emphasizes efficiency, and achieves near real-time recognition times. Scale Invariant Feature Transform (SIFT) (David G. Lowe 2004) is a feature-based image matching approach, which lessens the damaging effects of image transformation to a certain extent. Features extracted by SIFT are invariant to image scaling and rotation, and partially invariant to photometric changes. SIFT mainly covers 4 stages throughout the computation procedure as follows:

- **Local extremum detection:** first, use difference-of-Gaussian (DOG) to approximate Laplacian-of-Gaussian and build the image pyramid in scale space. Determine the keypoint candidates by local extremum detection.

- **Strip unstable keypoints:** use the Taylor expansion of the scale-space function to reject those points that are not distinctive enough or are unsatisfactorily located near the edge.

- **Feature description:** Local image gradients and orientations are computed around keypoints. A set of orientation, scale and location for each keypoint is used to represent it, which is significantly invariant to image transformations and luminance changes.

- **Feature matching:** compute the feature descriptors in the target image in advance and store all the features in a shape-indexing feature database. To initiate the matching process for the new image, repeat the above steps and search for the most similar features in the database.

SIFT features are local features and are mostly invariant to image translation, rotation, scale reduction and amplification, brightness changes, occlusion and noise, and are stable to visual changes and affine transformation to a certain extent. They
have high distinctiveness and abundant information, and provide fast and exact matching in a large feature database. The computation of SIFT features is relatively fast and optimized; thus, the SIFT matching algorithm may meet the need for real-time operation. Extensibility is strong and may combine conveniently with other feature vectors. In addition, the dimensionality of the descriptor is also very important, because it heavily influences the complexity of the matching process (at runtime) and the memory requirements for storing the descriptors.

3.4.2.1 Implementation of face recognition using SIFT

The main goal of this implementation is to reduce the computational costs involved in the authentication phase as well as to get more improved results. The proposed method is developed to combine the facial features with any other biometric traits to improve the performance of security. Hence development of an efficient authentication system based on hybrid features become great demand in most of the real time authentication based applications.

A face recognition system is an automatic generation of class id for feature selection, feature extraction and matching in SIFT which results in combining face with any other biometric traits. The face images must be collected into sets: every set (called "class") should include a number of images for each person, with some variations in expression and in the lighting. When a new input image is read and added to the training database, the number of classes called “class id” is required. Otherwise, a new input image can be processed and confronted with all classes present in database. The proposed method chooses a number of eigenvectors M' equal to the number of classes. Input image should be selected before starting image processing. This image can be successively added to database (training) or, if a database is already present, matched with known images. The class id is used to ensure the person face identification. Then the identification of the process is stored with the same class id for evaluation and it recognizes the entire process using scale invariant feature transform. If you choose to add image to database, a positive integer (face ID) is required. This positive integer is a progressive number which identifies a person (each person corresponds to a class). The SIFT algorithm helps to
identify the processing time involved in finding the feature descriptors. The procedure for face recognition work is based on the following steps.

Step 1: Select a face image of a person from the database
Step 2: Assign class id
Step 3: Store it in the database
Step 4: Repeat the step 1 to 3 for selecting another image
Step 5: Implement SIFT for retrieving the features
Step 6: Compare the feature index of both images

The first stage of calculation is to search over all scales and image locations. The Difference-of-Gaussian function is used to detect stable keypoint locations in scale space. The invariant detected location of images are subjected to change in scales that are searched with the same features deployed in all potential scales, using a constant function of scale which is well-known as scale space.

The invariant scale implementation uses gauss function efficiently to scan the likely points based on scale and orientation. This stage attempts to find those locations and scales that are identifiable from different views of the same object. This can be efficiently achieved by using a scale space function. Furthermore, it has been shown under reasonable assumptions that it must be based on a Gaussian function. Scale-space of an image, \( L(x, y, \sigma) \), is defined as:

\[
L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)
\]  \hspace{1cm} (3.6)

Where * is the convolution operator, \( G(x, y, \sigma) \) is a variable-scale Gaussian, and \( I(x, y) \) is the input image. The parameter \( \sigma \) is the scale of the keypoint and is also the standard deviation of the Gaussian function. The sequence of scales is called an octave. As shown in Figure 3.9, the octave scale space (Krystian Mikolajczyk and Cordelia Schmid 2004) construct the primary images that are subjected to Gaussian approach and produce set of image space with different Gaussian function by depreciating the images.
The construction of $D(x, y, \sigma)$ is illustrated in Figure 3.10. The input image is incrementally convolved with Gaussian function. This produces images separated by a constant $k$ in scale space, shown in the left stacks. The convolved images are grouped by octave, where an octave corresponds to doubling the value of $\sigma$. Each octave is divided into an integer number, $s$, of intervals, so that $k = 2^{1/s}$. For the final extremal detection to cover a complete octave, it is necessary to produce $s + 3$ Gaussian blurred images in the left stacks. The Gaussian image with twice the initial value of $\sigma$ is the image of two images from the top of the stack. After processing a complete octave, a new image is made from resampling this image to half its size. The new image becomes the first image of the next octave. The right side stack shows the Difference-Of-Gaussian (DOG) images, the result of subtracting adjacent image scales in the left stack.

To efficiently detect stable keypoint locations in scale-space, the proposed system using scale-space extrema in the Difference-of-Gaussian function convolved with the image, $D(x, y, \sigma)$. This can be computed from the difference of two nearby scales separated by a constant $k$:

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y)$$ (3.7)
\[
= \left( L(x, y, k\sigma) - L(x, y, \sigma) \right)
\]

The Gaussian image represented by

\[
G = k \ast \sigma
\]

The proposed method is implemented in the following selected images, and the identification was done by creating a class id. The class id will identify the face and create patch. The patch is stored in image database. Based on the selection of an image in the portal from database, a class id is created with a positive integer value less than 5. The process is repeated for selecting an image which is either totally different or the same image with different posture.

Figure 3.10 Comparison of sample point with neighbour to detect local extrema using SIFT

From Indian face database (IITK) there are many data sets have been taken for comparison. These image sets are compared and it performs the face recognition using SIFT.

In order to detect the local extrema of \( D(x, y, \sigma) \), each sample point is compared to its eight neighbours in the current image and its nine neighbours in the scale above and below. Here, Figure 3.10 shows comparisons of sample point with
neighbour to detect local extrema using SIFT, and it transforms image data into scale-invariant coordinates relative to local features. These scale-invariant coordinates are represented by feature descriptors.

A point is selected as a candidate keypoint only if it is larger than all of its neighbours or smaller than all of them. Figure 3.11 Pixel comparisons to detect nearest image of difference-of-Gaussian Images (Guo et al. 2010).

![Figure 3.11 Illustration of pixel comparisons to detect nearest image of DOG](image)

The SIFT feature is applied to such image data set for further recognition process. The nearest image can be traced using SIFT feature comparison considering the boundary of SIFT region. To estimate the distance compare the two image sets where one is the source and other is the destination.

\[
d(x, y) = \sqrt{\sum_i (x_i - y_i)^2} \tag{3.10}
\]

Where, \(i = 1\) to \(n\); if the distance has to be calculated within SIFT block then

\[
d(x, y) = \sum_i |x_i - y_i| \tag{3.11}
\]

If the feature has to be traced within the SIFT region then

\[
d(x, y) = \frac{xy}{\|x\|\|y\|} \tag{3.12}
\]
Such method will detect nearest neighbour by considering SIFT as the major factor. In the above formula \( \| x^2 \| \| y^2 \| \) is the distance between two features, maximum the distance within images deal with maximum deviation and minimum results in the close feature comparison.

3.4.2.2 Results and Discussion

The proposed method using SIFT algorithm is reliable and efficient for authentication process. It is used for categorizing every image captured and further stored in the image database. It makes the similarity analysis of face and any other biometric traits combined together to authenticate a person. The key point detector of SIFT combines the detector of face and any biometric trait and it makes fixed detector points in the training image data sets.

![Figure 3.12 Matched pairs of SIFT features between same and alternate images of different class value](image)

Different Gaussian filters are applied on the various key point detectors with difference in scales. Figure 3.12 shows the SIFT comparison between same and alternate images of different class value.
The biometric sample template and the stored template are compared during authentication and the level of similarity or a matching score is generated. Typically, the higher the score value represents a higher probability that the two biometric measurements come from the same person.

The aim of this face recognition system is to measure similarity between query face image with all face images of database and retrieve the image which has got highest similarity i.e. nearest neighbour. Since query is created from one of the database images (source or original image), the method should retrieve that specific original face image. SIFT provides better results on face trait. Two sets of images are compared and feature extraction is done using SIFT extraction method. After comparing the image sets the SIFT generates the class mean value of two image data sets. Figure 3.13 shows the class mean value of two image data sets.

![Figure 3.13 Illustration of Class mean value of image data sets](image)

The results in terms of class mean value, distance, scale space value for the above mentioned images (using image data sets 1 and 2 taking only sample images) are as follows,

- The nearest class number is : 1
- With a distance : 1.6053e+008
- The distance from face space is : 2.0339e+012
Detecting locations that are invariant to scale change of the image can be accomplished by searching for stable features across all possible scales, using a continuous function of scale known as scale space. Table 3.3 shows the comparison of SIFT based existing system and proposed system.

Table 3.3 Comparison of SIFT based existing Unimodal and Multimodal system with proposed method

<table>
<thead>
<tr>
<th>Biometric Traits</th>
<th>False Reject Rate (in %)</th>
<th>False Accept Rate (in %)</th>
<th>EER (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face and Fingerprint (Bagal et al. 2013)</td>
<td>10-20</td>
<td>3-5</td>
<td>3.65</td>
</tr>
<tr>
<td>Face identification by SIFT-based Complete Graph Topology (Dakshina Ranjan Kisku et al. 2007)</td>
<td>10-13</td>
<td>4-6</td>
<td>4.29</td>
</tr>
<tr>
<td>Fingerprint and Iris with Cryptography (Balakumar and Venkatesan 2011)</td>
<td>10</td>
<td>2</td>
<td>1.12</td>
</tr>
<tr>
<td>Face Skin Detection Based Cryptography in Steganography (SDBCS) (Surendiran and Alagarsamy 2010)</td>
<td>20</td>
<td>5</td>
<td>6.73</td>
</tr>
<tr>
<td>Face and SIFT (Proposed method)</td>
<td>10</td>
<td>1</td>
<td>0.98</td>
</tr>
</tbody>
</table>

The above Table 3.3 shows and proves that the face recognition system using SIFT provides better result compared to other existing methods. Also it provides strong security to the information. In contrast to the significant effort to build very large face databases, there is not a unique standard protocol to evaluate performances. Face recognition algorithm performance is typically characterized by
correct identification rate, FAR (False Acceptance Rate) or FRR (False Rejection Rate) under closed-world assumptions (Daniel Riccio and Gabriele Sabatino 2007).

False Reject Rate (FRR). One of the problems that can occur is called false rejects. A false reject is the situation where a valid user tries to authenticate and is falsely rejected by the system.

False Accept Rate (FAR). The second type of error a biometric system is to make false accept. In contrast to false rejects, a false accept means that a user is successfully accepted (authenticated) even though he/she should have been rejected.

To implement in e-voting application there are actually two scenarios where it can be about false accepts (Table 3.3).

- An unauthorized user is erroneously accepted for a vote
- An authorized user is confounded with another valid user

If a biometric device is used as an access control mechanism, a false reject may be acceptable, as it may only require the user to use a different means of authentication. In the context of e-voting, a false reject means to deny an individual of the possibility to execute his/her right as a citizen. The existing methods are used to calculate a coefficient matrix using all training samples to represent the test sample, and choose a certain number of neighbours to classify the test sample. These methods were effective on many face databases; however, it costs a large amount of time to calculate the coefficient matrix in practice. From the proposed method it is proven that any online web based application domain is very easy to access and it provides the highest level of security when it is implemented using SIFT on biometric traits.

3.4.2.3 Dataset and System Requirement

The database contains a set of face images taken in February, 2002 in the IIT Kanpur campus. There are eleven different images of each of 40 distinct subjects. For some subjects, some additional photographs are included. All the images were taken against a bright homogeneous background with the subjects in an upright,
frontal position. The files are in JPEG format. The size of each image is 640x480 pixels, with 256 grey levels per pixel. The images are organized in two main directories - males and females. In each of these directories, there are directories with name as a serial numbers, each corresponding to a single individual. In each of these directories, there are eleven different images of that subject, which have names of the form abc.jpg, where abc is the image number for that subject. The following orientations of the face are included: looking front, looking left, looking right, looking up, looking up towards left, looking up towards right, looking down. Available emotions are: neutral, smile, laughter, sad/disgust.

SIFT and its variants are implemented in Matlab 2008 and executed on a Dell PC. It has a Pentium(R) Dual-Core CPU @2.60GHz, and 4G memory, running Windows 7. In order to conduct empirical comparative analysis of SIFT and its variants, proposed method used image data sets which is provided by Indian face database – IIT, Kanpur. Within the data sets, a set of images are used to test scale and rotation invariance, blur invariance, illumination invariance, and affine invariance.

From the above implementations, which are discussed in subsection 3.4.1 and 3.4.2 respectively, it is strongly recommended that a face biometric trait provides better accuracy and recognition rate compared to other existing biometric traits. Unimodal Biometric Authentication System (UBAS) is not adequate for authentication because of its low security. So, the research focuses on Multimodal Biometric Authentication System (MMBAS), to combine face and finger print and applying steganography algorithm for data security using Bit Plane Complexity Segmentation (BPCS) method and Discrete Wavelet Transform (DWT).

3.4.3 A combination of face and finger print authentication system

The proposed method combines the face and finger print trait and conceal the information using steganography method. Steganography based techniques can be suitable for transferring critical biometric information from a client to a server. There are two application scenarios where hiding method is the same, but differ in
the characteristics of the embedded data, host image and medium of data transfer (Jain and Uludag 2003).

3.4.3.1 Face Recognition System

Steganography is an ancient art of conveying messages in a secret way such that only the receiver knows the presence of the message. The message is hidden in another media such that the transmitted media appears meaningful to the attacker. If the hidden message is extracted the steganography technique fails. Steganographic technique allows one party to communicate with another party without third party being aware that communication is occurring. Steganography is the method of encoding secret data such that the existence of the information is concealed. Usually, the data is concealed inside a protected cover such that even if hostile agents discover the cover, there is no suspicions about the presence of data in that cover (Shrikant S Khaire and Sanjay L Nalbalwar 2010). However, Cryptographic and Steganographic techniques differ from each other. In cryptography, the original message is scrambled i.e. its original structure is changed in order to make it meaningless. Thus, when an attacker discovers the message it is still difficult for him to get the original message back. Cryptography does not try to hide the message. In steganography, the message is secretly hidden inside an image or audio/video file. Thus there arises no suspicion to the attacker. Steganography does not attempt to scramble the original message. There are basically three types of Steganographic protocols:

- **Pure – key steganography:** In this model, there requires no exchange of stego – key. This method is the simplest but is the most insecure means to communicate secretly.

- **Secret – key steganography:** In this model, both sender and receiver shares common secret – key before conveying messages.

- **Public – key steganography:** In this model, two keys are required; one is public key and the other is private key. The public key is used for embedding message while the private key is used for extracting message.
The message ‘M’ is the secret data that the Sender wishes to hide without any suspicion. The secret data can be audio, video, image, text. The cover ‘X’ is the original image, audio file, video file, in which the secret message ‘M’ is to be embedded. The cover ‘X’ is also called as “Message Wrapper”. It is not necessary that the cover ‘X’ and the message ‘M’ should have homogeneous structure. For example, text message or an audio file can also be hidden into video or image. In this proposed system cover ‘X’ and Message ‘M’ are images.

![Illustration of basic digital Steganography encoder](image)

**Figure 3.14 Illustration of basic digital Steganography encoder**

Figure 3.14 show that Stego-image ‘Z’ is the image in which secret image ‘M’ is embedded. It should be ensured that at any point, the Stego-image should resemble the cover image else it will cause suspicion. Stego-key ‘Z’ is provided to the receiver so that only he can be able to extract the secret image from the cover image (Bloisi and Locci 2007).

In cryptographic approach the proposed method has determined the identity proof for the voters using hashing algorithms (MD5 and SHA1) through internet. From those results it finds that, security is not sufficient for the data. Also the content binding is time consuming. So, to overcome this problem, the steganography technique is used for data hiding (Hamid A Jalab and Zaidan 2010). To ensure the election accuracy, different methods have been proposed for hiding information.

The proposed work focuses on basic steganography and various characteristics necessary for data hiding. This technique is called Bit Plane
Complexity Segmentation (BPCS) Steganography. The proposed method uses BPCS method for a single text or a binary image which is automatically scattered and embedded in video frames with genetic distortion audio tracks and text image with automated dynamic key for every transaction. BPCS steganography was introduced to overcome the short comings of traditional Steganographic techniques such as Least Significant Bit (LSB) technique, Transform embedding technique, Perceptual masking technique (Shrikant S Khaire and Sanjay L Nalbalwar 2010). These traditional techniques have limited data hiding capacity and they can hide up to 10 – 15% of the data image amount. BPCS steganography makes use of important characteristic that of human vision. In BPCS, the data image is divided into “informative region” and “noise-like region” and the secret data is hidden in noise blocks of data image without degrading image quality (Shrikant S Khaire and Sanjay L Nalbalwar 2010). In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits (Habes 2005). But in BPCS technique, data is hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region.

- Complex areas that would appear as noise-like seeming regions in each bit-plane can then be replaced with the hidden data, which ideally is also noise-like

- In bit-plane complexity segmentation Steganography, a complexity measure is introduced to decide whether a binary image is noise-like or not

![Illustration of binary image patches using BPCS](image)

(a) Noise like patch  (b) Informative patch

Figure 3.15 Illustration of binary image patches using BPCS
In BPCS, a multi-valued image (P) consisting of n-bit pixels can be decomposed into a set of n – binary pictures. Ordinary image data is represented by a pure binary code system which is commonly used in image processing. However CGC is preferred over PBC in BPCS steganography. Example: P is an n-bit grey image say n=8. Therefore P = [P7 P6 P5 P4 P3 P2 P1 P0] where P7 is the MSB bit plane and P0 is the LSB bit plane. Each bit plane can be segmented into “informative” and “noise” region. An informative region consists of simple pattern while noise-like region consists of complex pattern. In BPCS, the proposed method replaces each noise-looking region with another noise-looking pattern without changing the overall image quality.

This technique involves reducing the number of grey levels in the image. Thus reducing the number of bits required to hold an image. Let P be the number of pixels in an original image to be compressed to N grey levels. Create a histogram of the grey levels in the original image. Identify N ranges in this histogram that approximately P/N pixels lie in each range. Identify the median grey level in each range. Clearly, a loss of information has gone on but this has been minimized by ensuring that the groupings are as equal as possible. After this operation key and information is placed in this resultant image. Figure 3.16 shows the redundant data identification by shared secret key in Steganographic method.

Figure 3.16 Illustration of redundant data identification by shared secret key
A data hiding method, which is applicable through steganography, and the biometric concepts provide full security for data that is passed through the network from different places. The proposed method supports a remote voter registration scheme that increases the accuracy of the current system. In this scheme the voter identification is carried out by biometric systems. This method provides how to take advantage from the most usable biometrics to carry out the voter registration process in a more effective way. This modification ensures higher payload and security. The main principle of BPCS technique is that, the binary image is divided into informative region and noise-like region. The secret data is hidden into noise-like region of the data image without any deterioration (Shrikant S Khaire and Sanjay L Nalbalwar 2010). This explains voting through internet, with facial detection integrated with finger print authentication and automated load balancing, fused with data hiding security.

The proposed method is used to build a system program that is able to hide data in digital video files, more specifically in the images or frames extracted from the digital video file MPEG (Sujay Narayana and Gaurav Prasad 2010). The compressed method of embedding the data into various cover media plays a major role in transferring the data in the network. The users need not choose the cover media in which the data is to be hidden (Rengarajan Amirtharajan and Jithamanyu 2010). Choice of cover media is automatically done with dynamic allocation. Each and every transaction in cover media changes according to the data.

The proposed method has been developed a web site using ASP.NET and in that the registration option is provided to the voter. The voter must fill up the registration form and then automatically the webcam will be switched on and the voter’s face will be captured. The voter should also place their finger print in registration process itself. The details of the voter are sent to the election commission server. In biometric system the information hiding is very important, so, the proposed method has introduced a concept of steganography to provide more security to the data. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. Information hiding is a technique to keep information secured using redundant cover data such as
images, audios, movies, documents, etc. This technique has recently become important in a number of application areas (Mazurczyk et al. 2010).

As a result, the proposed method briefly addresses the following problems of substitution techniques of audio steganography (Qingzhong Liu et al. 2008 and Ru et al. 2006).

- Transparency - evaluates the audible distortion due to signal modification like message embedding or attacking.
- Robustness - measures the ability of embedded data to withstand against intentional and unintentional attacks.
- Capacity - refers to the ability of a cover media to store secret data, and it can be measured by the amount of secret data (bytes) that can be hidden in a byte of a cover media.

Problem 1: Having low robustness against attacks which try to reveal the hidden message. In samples LSBs are more suspicious, thus embedding in the bits other than LSBs could be helpful to increase robustness.

Problem 2: Having low robustness against distortions with high average power.

The Solution

Accordingly, there are two following solutions for above mentioned problems:

- The solution for first problem: Making more difficult discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples.

- The solution for second problem: Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.
To integrate these two solutions, “embedding the message bits in deeper layers” that is a part of second solution also can satisfy “modifying the bits else than LSBs in samples” of second solution (Saurabh Singh and Gaurav Agarwal 2010). In addition, when trying to satisfy “other bits alteration to decrease the amount of the error” of second solution, if it ignore the samples which are not adjustable, also “selecting not all samples” of first solution will be satisfied. Thus, the algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. The following section explains the algorithmic approach of the proposed system.

a. Algorithmic Approach

Using this algorithm the data can be hidden in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. The data should not be hidden in LSB bits. The hackers will mostly search the data in LSB bits. So, the steganography algorithm will help to store the data into the darkest area of the image which is considered as a removal part of the image. The algorithmic approach of the method is described as follows,

- Alteration

At the first step, message bits are substituted with the target bits of samples. Target bits are those bits which place at the layer that the proposed method want to alter. This is done by a simple substitution that does not need adjustability of result being measured.

- Modification

In fact this step is the most important and essential part of algorithm. All results and achievements are depending on this step. In this stage algorithm tries to decrease the amount of error and improve the transparency. The World Academy of Science, Engineering and Technology have used two different algorithms. First one is simpler like ordinary technique, but it is efficient to modify the bits of samples better. Since transparency is simply the difference between original sample and
modified sample, with a more intelligent algorithm, the proposed algorithm will try to modify and adjust more bits and samples than some previous algorithms (Szczypiorski and Mazurczyk 2007). If the proposed algorithm can decrease the difference of them, then the transparency will be improved. There are two cases shown with examples as shown below.

Example 1

Sample bits are: $00101111 = 47$

Target layer is 5, and message bit is 1

Without adjusting: $00111111 = 63$ (difference is 16)

After adjusting: $00110000 = 48$ (difference will be 1 for 1 bit embedding)

Example 2

Sample bits are: $00100111 = 39$

Target layers are 4&5, and message bits are 11

Without adjusting: $00111111 = 63$ (difference is 24)

After adjusting: $00011111 = 31$ (difference will be 8 for 2 bits embedding)

It is clear, that the most transparent sample pattern should be measured fittest. It must be considered that in crossover and mutation the place of target bit should not be changed.

➢ Verification

This stage is act like quality controller. What the algorithm could do has been done, and now the outcome must be verified. If the difference between original sample and new sample is attachable and reasonable, the new sample will be accepted; otherwise it will be rejected and original sample will be used in reconstructing the new file instead of that new sample.
Reconstruction

The last step is new steganography file creation. This is done sample by sample. There are two states at the input of this step. Either modified sample is input or the original sample that is the same with host file. The proposed method can claim the algorithm does not alter all samples or predictable samples. Using the proposed algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness. The following steps explain the proposed algorithm for steganography process.

Step1: Read the information from the file and encrypt the message through the public or private key

Step2: Read the image file and Compress the image by the Quantizing technique

Step3: Compute the threshold (T), based on average grey value and place the key information in the image where value>T

Step4: Send through internet to the Destination and Decompress image and extract key information

Often the storing of data pattern should be changed as image, text, audio or video bit (Qingzhong Liu et al. 2008 and Ru et al. 2006). When there are many numbers of voters to be registered, they can be accommodated using the proposed system by taking only one bit pattern from their face or fingerprint based on the concept of interoperability. The details of the patterns of the voter can be stored in database. If the voter is already registered the system will show the message that “Voter is already registered”. So, the duplication of the voter information can be avoided. Then based on the given voter information the voter will be verified through this algorithm and with election commission server. If it is matching, then the voter details can be displayed on the screen. In server side system the administrator can take care of the verification.
Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image feature extraction lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. When an image is decomposed into bit-planes, the complexity of each region can be measured. Areas of low complexity such as homogenous color or simple shapes appear as uniform areas with very few changes between one and zero (Walaa Abu-Marie et al. 2010 and Prosanta Gope et al. 2010). Complex areas would appear as noise-like regions with many changes between one and zero. These random seeming regions in each bit-plane can then be replaced with hidden data, which is ideally also noise-like. Because it is difficult for the human eye to distinguish differences between the two noise-like areas, are able to disguise the changes to the image. In BPCS steganography, a complexity measure is introduced to decide whether a binary image is noise-like or not. The complexity measure currently used is defined based on the length of non-edge border between zero and one. The functions of the proposed approach are:

- Read Frames
- Select Frame
- Hide the Data
- Read Frames Sequence
- Extract the Data

The proposed method is used to build a system program that is able to hide data in digital video files, more specifically in the images or frames extracted from the digital video file MPEG (Sujay Narayana and Gaurav Prasad (2010) and Seunglim Yong 2007). The combination of face and fingerprint authentication system is implemented and it provides security for the large number of users. The main idea in developing this system is to authenticate the genuine voter in an efficient way. The steganography method is to hide data in mathematical functions that are in compression algorithms. There are two functions can be used in validation process. They are Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) respectively. The validation process takes place in
face recognition phase. So, the proposed face detection method uses the Discrete Wavelet Transform (DWT) method to identify the person. There are three modules involved in the proposed face recognition method they are,

- Wavelet sub band extraction using Discrete Wavelet Transform (DWT)
- Face Localization
- Face Segmentation

The registration proof is generated by means of this phase. Such proof is generated with the biometric information provided by the voter.

![Diagram of Module I, II, and III](image)

**Figure 3.17 Illustration of proposed face recognition using Discrete Wavelet Transform**

Face localization extract the ALL subband of the \( C_r \) component that carries the skin color information from \( L_r \) proposed system generate a threshold value for the \( C_r \) component in wavelet domain and use it to filter out the non-skin area. To avoid wrong face region detection, simple morphological operations are used to fill (dilation) in any small hole in the facial area and to remove (erosion) any small object in the background area. To generate a threshold value for the \( C_r \) component for skin color in wavelet domain, proposed method has investigated the wavelet
coefficients values in the $C_r$ of the ALL wavelet sub band and found that there is a threshold value that can differentiate the face region and the background.

The face region is denoted as $O_1$ from the background. This method is derived using simple constraints of the location of the face region in the image frames. The proposed method used rectangles with certain aspect ratio and found that the aspect ratio of the bounded rectangles of 1:2 is most suitable for the image frames tested. The encoder compresses the input image using wavelet decomposition and encodes the image information to elementary stream. This data stream will then be inverse quantized and the inverse wavelet transform will reconstruct the data to images. Then face recognition methods will be applied on the image for facial feature extraction.

Figure 3.18 shows a conventional face recognition system in compression domain. Figure 3.19 shows the block diagram of a desired face recognition system in compression domain.

Figure 3.18 Illustration of a conventional face recognition system in compression domain
Figure 3.19 Block diagram of a desired face recognition system in compression domain

Discrete Wavelet Transform is applied on the images to encode the DWT coefficients. This is a concept of one dimensional DWT filters applicable in 2-dimensional way because images are 2-D signals. \( \Psi \) (PSI), \( \varphi \) (PHI) are the wavelet filters applied on the column and row respectively. The LL, LH, HL, HH are defined LL as average, LH as intensity variations along columns (Horizontal edges), HL as intensity variations along rows (Vertical edges), HH as intensity variations along diagonals respectively. Table 3.4 shows the single level coefficients of wavelet subbands.

<table>
<thead>
<tr>
<th>LL</th>
<th>HL</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH</td>
<td>HH</td>
</tr>
</tbody>
</table>

LL – LOW pass filter horizontally and LOW pass filter vertically

\[
\varphi (n_1,n_2) = \varphi(n_1),\varphi(n_2) \quad (3.13)
\]

HL – HIGH pass filter horizontally and LOW pass filter vertically

\[
\Psi H (n_1,n_2) = \Psi(n_1),\varphi(n_2) \quad (3.14)
\]

LH – LOW pass filter horizontally and HIGH pass filter vertically

\[
\Psi V (n_1,n_2) = \varphi(n_1),\Psi(n_2) \quad (3.15)
\]
HH – HIGH pass filter horizontally and HIGH pass filter vertically

$$\Psi D (n_1, n_2) = \Psi(n_1), \Psi(n_2)$$

(3.16)

The ALL and ALH wavelet subbands will be extracted directly after the inverse quantization. Further wavelet decomposition of ALL to HALL and ALH to AALH form a face recognition system. In the desired system, the inverse wavelet transform is omitted and hence the computational complexity is reduced. Table 3.5 shows the multilevel coefficients of wavelet subbands.

<table>
<thead>
<tr>
<th>ALL</th>
<th>HLL</th>
<th>ALH</th>
<th>HLH</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLL</td>
<td>DLL</td>
<td>VLH</td>
<td>DLH</td>
</tr>
<tr>
<td>HL</td>
<td></td>
<td></td>
<td>HH</td>
</tr>
</tbody>
</table>

Whenever the coefficients are splitting up into two bands, the band width of signals gets halved in each of the subbands. So, \(n/2\) samples are required.

![Figure 3.20 Scaling function of wavelet sub band using Discrete Wavelet Transform](image)
It is employed to select the two sets of wavelet subbands and these wavelet subbands are extracted after the inverse quantization in the compression system for face recognition. Figure 3.20 shows scaling function of DWT. Thus the face recognition is successfully implemented.

3.4.3.2 Finger Print Authentication System

Fingerprint Authentication System provides security for the users large in number. The main idea in developing this system is to authenticate a person in an efficient way. After detecting the face, the module II has to be implemented. A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification. The manual approach for fingerprint recognition by experts is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based.

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person’s identity by his fingerprint(s). The fingerprint identification system tries to match his fingerprint(s) with the whole fingerprint database, without the knowledge of the person’s identity. It is especially useful for criminal investigation cases, and it is the design principle of AFIS (Automatic Fingerprint Identification System).

However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint. As long as the representation of fingerprints is unique, the fingerprint matching is either for the 1-to-1 verification case or 1-to-n identification case, it is
straightforward and easy. The following modules are involved in the proposed method of fingerprint authentication.

- Pre-Processing
- Minutiae Extraction And Storage
- Minutiae Matching

For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user’s finger is too dirty or dry. However, the testing database for the proposed work is from the available fingerprints provided by FVC2004 (Fingerprint Verification Competition 2004). So no acquisition stage is implemented. However, as shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by minutiae, which are some abnormal points on the ridges. Among the variety of minutiae types reported in literatures, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive. Since various data acquisition conditions such as impression pressure can easily change one type of minutiae into the other, most researchers adopt the unification representation for both termination and bifurcation. So each minutia is completely characterized by the parameters, namely, x-coordinate, y-coordinate and orientation.

Fingerprint bifurcation is to transform the 8-bit grey fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows with white. The following Figure 3.21 shows the fingerprint detection system flow diagram.
To extract thinned ridges from grey-level fingerprint images directly, the proposed method traces along the ridges having maximum grey intensity value. However, binarization is implicitly enforced since only pixels with maximum grey intensity value are remained. Figure 3.22 shows the minutiae point extraction of finger print from database for matching.

Figure 3.21 Flow diagram of finger print authentication system

Figure 3.22 Minutiae points extraction from finger print image
Also in testing, the advancement of each trace step still has large computation complexity although it does not require the movement of pixel by pixel as in other thinning algorithms. After implementing module II the proposed method finds the new MMBAS.

3.4.3.3 Results and Discussion

The proposed method implementation which deals with digital images that are acting as a cover medium to store secret data in such a manner that becomes undetectable. Hence it provides a very high means of security without suspicion. The following is the approved voter registration form which allows the voters to register themselves in an e-voting application through internet. Once the registration process is over the voter information is stored in the database. That means a biometric characteristic can give at the same time both authentication and integrity to the contents.

In the proposed method there are two biometric traits (face and finger print) has been used to develop a Multimodal Biometric Authentication System (MMBAS). In face recognition system the proposed method obtained the following result after implementing the methods BPCS steganography and Discrete Wavelet Transform (DWT) which shows in Figure 3.23. The values for face have been obtained by using the images in local database. This proposed method will protect the contents of the voter registration by binding the information. The multiband feature fusion method is employed to select the two sets of wavelet subbands. These wavelet subbands are extracted after the inverse quantization in the compression system for face recognition.
In face recognition module using DWT algorithm the dimensionality of image is reduced so it is used for image compression, feature extraction process. This algorithm decomposes the image into 4 subband (sub image) i.e., LL, LH, HL, HH. The output extracts the detailed output of input image. LL is the approximate image of input image it is low frequency subband so it is used for further decomposition process. LH subband extract the horizontal features of original image HL subband gives vertical features HH subband gives diagonal features LH, HL, HH are high frequency subbands.

After successful implementation of proposed face module, the finger print module is implemented using a locally adaptive binarization method which is used to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs to. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutiae in the bound region are confusing with those spurious
minutiae’s that are generated when the ridges are out of the sensor. Figure 3.24 shows illustration of minutiae matching process between registered fingerprint.

Figure 3.24 Illustration of minutiae matching process between registered fingerprint

After comparing the minutiae points between the registered fingerprint, the proposed method extracts the matched minutiae points from those fingerprints as templates and it founds the matched fingerprint. Figure 3.25 shows the illustration of minutiae point extraction from different fingerprints for matching process.

Figure 3.25 Illustration of minutiae point extraction from different fingerprints for matching
Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. An iterative, parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans.

In proposed method the steganography is applied to digital images, because, the digital images are an array of numbers that represent light intensities at various points (pixels). Images can have 8 bits per pixel or 24 bits per pixel. With 8 bits/pixel, there are 28, or 256, color varieties. With 24 bits/pixel there are 224, or 16,777,216, color varieties. Color variation for a pixel is derived from 3 primary colours: red, green and blue.

The 24 bit images use 3 bytes to represent a color value (8 bits = 1 byte)
1 pixel = (00100111 11101001 11001000)
          red     green     blue

The idea behind the BPCS algorithm is to insert the bits of the hidden message into the least significant bits (LSB) of the pixels. Simplified with a 24 bit pixel:

1 pixel:
     (00100111 11101001 11001000)
Insert 101:
     (00100111 11101000 11001001)
          red     green     blue

Simplified with an 8 bit pixel:

1 pixel:
     (00  01  10  11)
      white  red  green  blue
Insert 0011:
     (00  00  11  11)
      white  white  blue  blue
The least significant bit insertion method is probably the most well known image steganography technique. It is a common, simple approach to embedding information in a graphical image file.

For example, the letter A can be hidden in three pixels. Assume the original three pixels are represented by the three 24-bit words below:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

The binary value for the letter A is (10000011). Inserting the binary value of A into the three pixels, starting from the top left byte, would result in:

(00100111 11101000 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)

If a biometric device is used as an access control mechanism, a false reject may be acceptable, as it may only require the user to use a different means of authentication.

Table 3.6 Comparison of Steganography based existing and proposed multimodal system

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>FRR (in %)</th>
<th>FAR (in %)</th>
<th>EER (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speech &amp; Signature Feature Level Fusion approach (Dapinder Kaur et al. 2013)</td>
<td>10-30</td>
<td>2-10</td>
<td>3.54</td>
</tr>
<tr>
<td>Face, Palm print &amp; Canonical Form based approach (Nageshkumar et al.2009)</td>
<td>10</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Face &amp; Finger Print Steganography and DWT approach (Proposed method)</td>
<td>15</td>
<td>2</td>
<td>1.65</td>
</tr>
</tbody>
</table>
Table 3.6 shows the comparison of FRR, FAR and EER of existing and proposed biometric system in MMBAS. In the context of e-Voting, a false reject means to deny an individual of the possibility to execute his/her right as a citizen. From the proposed system it is proven that the e-voting process is very easy to access using steganography method in MMBAS.

This proposed method is based on the face and finger print recognition to describe the authentication in real life. Biometric characteristics cannot be lost or forgotten and are extremely difficult to copy, share and distribute. It requires the person to be present physically. The proposed method identified that face recognition seems to be a good compromise between reliability and social acceptance and balances security and privacy well. It requires minimal user interface. Fingerprints are reliable and non-intrusive, but not suitable for non-collaborative individuals. This has problems including presentation of fingerprint, elasticity of the skin, pressure, bad quality fingerprint, and impostor attacks. This kind of security provides better authentication than any other method (Alok Kumar Vishwakarma and Atul Kumar 2011). The main drawback of this proposed method is the storage space. There is a necessity for storing all the feature descriptors of the enrolled images for future references. The size of these feature descriptors data will be greater than the original image dataset and the performance of the system will rapidly decrease with respect to the increase in enrolment in the database. Maintenance cost is very high. To improve the storage space and to reduce the computational cost, the research focuses on SIFT based algorithm to combine more than one biometric traits to propose a new MMBAS.

3.4.3.4 Dataset and System Requirement

The proposed method which was implemented in MMBAS used local database for face recognition. This grey-level frontal view face database comprises 100 images from 50 people. There are 30 females and 20 males, each of whom has two images (xa and xb) with different facial expressions. The xa images are used as gallery for training while the xb images as probes for testing. All the images are randomly selected from the local face database. The images contain different facial
expressions and illumination conditions for each subject. The image size is 243 × 320 pixels, and an average of 230 features is extracted for each image. The raw face images were used without any kind of pre processing (cropping, normalization, histogram equalization, etc.) to assess the robustness of the algorithms in the comparison.

For fingerprint acquisition, optical or semiconductor sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user’s finger is too dirty or dry. However, the testing database for the proposed work is from the available fingerprints provided by FVC2004 (Fingerprint Verification Competition 2004). So no acquisition stage is implemented. The details of all the datasets that have been used in this chapter are presented in Annexure I.

The biometric concepts are implemented using ASP.NET. The biometric evidence is received through the web cam (Song et al. 2008). The steganography algorithm is implemented using JAVA programs. This reduces the number of potential candidates to face biometrics, since these allow biometric information to be acquired by means of capturing the face and combine it with steganography. Face detection system provides nonintrusive way of authentication.

### 3.5 SUMMARY

Face recognition has a high identification or recognition rate of greater than 90% for huge face databases with well-controlled pose and illumination conditions. This high rate can be used for replacement of lower security requirement environment and could be successfully employed in different kind of issues such as multi-media. Automatic recognition is a vast and modern research area of computer vision, reaching from face detection, face localization, face tracking, extraction of face orientation and facial features and facial expressions. These will need to tackle some technical problems like illumination, poses and occlusions.

This chapter described about the implementation of first phase as face recognition system using SIFT feature descriptors and it analyzed the results with comparison. Also the combination of face, finger print, palm print, iris recognition is
readily available. All existing systems have their own limitations. There is no possibility of having the combination of face and finger knuckle. Compared to other existing biometric traits, finger knuckle is one of the most popular traits in current research. So, in proposed MMBAS the combination of face and finger knuckle traits are combined to provide better performance and accuracy to improve the security level. To propose a new MMBAS the FKP based system is implemented as the second phase of proposed method.