CHAPTER 2

REVIEW OF LITERATURE

2.1 GENERAL

Many methodologies were proposed in biometric field with a motive to hit upon the best combination technique that suit well to all application domains. Apart from newer techniques, innovations were made in biometric field by focusing on biometric traits, as it plays a vital role in improving the performance of biometric system. Scale Invariant Feature Transform (SIFT) algorithm, called SIFT descriptor, has been proposed by David G. Lowe (2004) and proved to be invariant to image rotation, scaling, translation, partly illumination changes. The investigation of SIFT features for biometric authentication has been explored in modern world. The basic idea of the SIFT descriptor is detecting feature points efficiently that identify stable points in the scale-space. This chapter discusses some of the methods in literature which served as the prime motive for carrying out this research work.

2.2 BIOMETRICS AND IMAGE SECURITY

The term biometric comes from the Greek word ‘bios’ which means life and ‘metrics’ means measure. It is well known that humans intuitively use some body characteristics which can be stored as images such as face, gait or voice to recognize each other. The importance of image security is most notable in biometrics. It consists of a series of methods for uniquely recognizing a subject (typically a human but can also be other animal). Biometric algorithms and procedures should confirm a system which ensures the identity of the target using biological traits: fingerprint, face image, DNA sequence, voice, walking gaits, etc. Many of these techniques are closely related to imaging science. Most of the biometric systems require strong security. Therefore, they usually make use of watermarking, cryptography, steganography and Scale Invariant Feature Transform (SIFT).
There are many properties listed in biometrics, they are as follows,

- Universality: Applicable to every human.
- Distinctiveness: Any two subject's biometric features must be sufficiently distinguishable.
- Permanence: The biometric features should be persistent over time. Obtaining or verifying them should not induce changes in the user's biometric features.
- Collectability: The features can be measured quantitatively.
- Performance: Accuracy, speed, low resource usage and invariability to environmental factors are desirable.
- Acceptance: It is important to measure the social acceptance of a certain biometric characteristic.
- Security: Biometric systems should ensure authenticity, integrity, privacy and resistance to attacks and forgery.

Securing the storage and transmission of images is one of the cornerstones of data security. Many biometric systems use imaging methods, and the need for secure biometrics storing and sharing schemes is increasing.

### 2.3 APPROACHES IN BIOMETRICS

The biometric authentication systems are best defined as measurable physiological and/or biological characteristics that can be utilized to verify the identity of an individual. They include fingerprints, retinal and iris scanning, hand geometry, voice patterns, facial recognition, gait recognition, DNA and other techniques. The biometric authentication system uses two kinds of approaches,

- Unimodal Biometric Authentication System (UBAS)
- Multimodal Biometric Authentication System (MMBAS)
Initially, these techniques were employed primarily in specialised high security applications; but compare to existing and proposed method, the benefit varies depends on the biometric trait used.

### 2.3.1 Unimodal Biometric Authentication System (UBAS)

Biometric systems based on single source of information are called Unimodal Biometric Authentication System (UBAS). This system considers the single biometric trait. Unimodal biometric systems rely on the evidence of a single source of information for authentication of person (Sanjekar and Patil 2013). Most biometric systems deployed in the real world are unimodal. It relies on a single biometric characteristic which could be hacked by the modern burglar (Thompson et al. 2010). Figure 2.1 shows the example of UBAS, which describes the finger print authentication system architecture.

![Figure 2.1 Example for UBAS (Finger print authentication system architecture)](image)

The above Figure 2.1 shows the fingerprint which is the unique skin structure of the finger. As a phenotypic biological feature it is unique, even for identical twins. The characteristic formation of the fingerprint normally doesn’t change over a person’s life span. For automatic processing, the fingerprint is taken using special sensor devices. In most cases the raw data taken is a grey scale image. To compare fingerprint images, a set of distinctive pieces of information is extracted from the grey scale images (Schimkea et al. 2005). These extracted features can be positions or configurations of ridge-lines, crossing, bifurcation and ending points, referred to as minutiae.
Unimodal system is usually more cost-efficient than a multimodal biometric system. However, it may not always be applicable in a given domain because of unacceptable performance and inability to operate on a large user population (Thompson et al. 2010). This system have many advantages, and it has to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates (Ross and Jain 2004).

- **NOISY DATA** - Susceptibility of biometric sensors to noise leads to inaccurate matching, as noisy data may lead to false rejection

- **INTRA CLASS VARIATION** - The biometric data acquired during verification will not be identical to the data used for generating template during enrolment for an individual. This is known as intra-class variation. Large intra-class variations increase the False Rejection Rate (FRR) of a biometric system.

- **INTER CLASS SIMILARITIES** - Inter-class similarity refers to the overlap of feature spaces corresponding to multiple individuals. Large Inter class similarities increase the False Acceptance Rate (FAR) of a biometric system.

- **NON UNIVERSALITY** - Some persons cannot provide the required stand alone biometric, owing to illness or disabilities (Golfarelli et al. 1997).

- **SPOOFING** - Unimodal biometrics is vulnerable to spoofing where the data can be imitated.

Some of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidence presented by multiple sources of information.

### 2.3.2 Multimodal Biometrics Authentication System (MMBAS)

Biometric system can also be designed to recognize a person based on information acquired from multiple biometric sources. Such system is known as Multimodal biometric system. Multimodal biometric system can offer substantial
improvement in the matching information. It is a combined and fusion methodology, the accuracy of which depends upon the adopted biometric trait from the person. It addresses the issue of non-universality or insufficient population coverage (Rupali L.Telgad et al. 2013). This system also effectively addresses the problem of noisy data. These systems also help in continuous monitoring and tracking of individual in situation when a single trait is not sufficient. Fusion schemes should be employed to combine the information presented by multiple biometric sources. There are various data combination levels that can be considered, examples are the feature level, score level and decision level (Fortuna et al. 2004).

Multimodal biometric integrates different biometric systems for verification in making a personal identification. This system takes advantage of the capabilities of each individual biometric. These systems can expect more accuracy due to the fact that they use multiple biometric modalities where each modality presents independent evidence to make a more informed decision. Multimodal biometric systems capture two or more biometric samples and use fusion to combine their analyses to produce a better match decision by simultaneously decreasing the FAR and FRR. All unimodal biometric systems can be used with combination of others to form a multimodal biometrics (Dapinder Kaur et al. 2013). For example:

- Speech and Signature
- Palm and Iris
- Face and Signature
- Face and Fingerprint

A biometric system which relies only on a single biometric identifier is often not able to meet the desired performance requirements. Ross and Anil K. Jain (2004) propose more than 10 multimodal biometric systems, which integrate face recognition, fingerprint verification, and speech verification in making a personal identification using different techniques. In their proposal the Principal Component Analysis (PCA) algorithm is used to extract the subspace of the images for feature matching using principal components. This subspace is called Eigen space. The face
and fingerprint is claimed by image acquisition model. Speech is extracted using speech acquisition model. During enrolment the features are extracted using Eigen space and Hidden Markov model (HMM) technique. Then it is compared with image templates for verification. Figure 2.2 shows the example of multimodal biometric authentication system using Eigen space and Hidden Markov model (HMM) techniques.

![Figure 2.2 Eigen space and Hidden Markov Model (HMM) in MMBAS](image)

The problems of traditional personal authentication systems may be solved by biometric systems. Biometric identification is extremely an effective authentication. It is an important weapon to protect against credit card fraud and phantom withdraws. Biometrics can identify a person’s unique physical characteristics, including fingerprints, facial features, voice pattern, retinal, irises DNA and keystroke (Bolle et al. 2001). The problem with biometrics approach is
that the biometric properties cannot reasonably be kept secret. Multimodal biometrics also address the problem of spoofing as it concern with multiple traits or modalities (Rupali L. Telgad et al. 2013), it would be very difficult for an imposter to spoof or attack multiple traits of genuine user simultaneously.

Many techniques were applied in UBAS and MMBAS for verifying and confirming a user’s identity. In which cryptography, steganography and Scale Invariant Feature Transform (SIFT) techniques are used to provide better authentication in a biometric system. A number of application domains are used in biometric systems. E-voting system is the challenging domain, where large amount of images have to be stored in the database for future use. These techniques namely Cryptography, Steganography and Scale Invariant Feature Transform (SIFT) are briefly discussed with suitable examples in this literature review, for both UBAS and MMBAS.

a) **Cryptography**

Biometric cryptosystems is a technique which combines biometrics and cryptography, and is popularly known as crypto-biometric systems. The integration of biometrics (Alexander P. Pons, and Peter Polak 2008) and cryptography is broadly carried out in two distinct steps. In case of biometrics-based key generation, a biometric matching along with an input biometric signal and a registered template are utilized in the release of the secret key.

Cryptography is one where security engineering and mathematics is joining together (Anderson et al. 2006). It is dependent on the secrecy of the secret or private key. The user chooses an easily remembered pass code that is used to encrypt the cryptographic key and this key is then stored in a database. It is the practice and study of hiding information. Cryptosystem is the combination of three elements: an encryption engine, keying information, and operational procedures for their secure use. There are three main types of cryptography symmetric, asymmetric and one-way cryptography (Hash) shown in Figure 2.3.
Figure 2.3 Types of Cryptosystems

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. Currently, the most commonly used hash functions are MD5 and Secure Hash Algorithm (SHA), with 128 to 512 bit output Digest Messages (DMs), respectively. It transforms a message of any length and computes a fixed length string. While for MD5, collision attacks are computationally feasible on a standard desktop computer (Klima 2005), current SHA-1 attacks still require massive computational power (Wang 2005), (around 269 hash operations), making attacks infeasible for the time being.

Many systems are proposed using cryptographic technique with Unimodal Biometric Authentication System (UBAS) and Multimodal Biometric Authentication System (MMBAS). Cryptographic hash functions play a central role in cryptology. A cryptographic hash function takes an input of arbitrary large size and returns a small fixed size hash value (Harshvardhan Tiwari and Krishna Asawa 2010). Cryptology is an important tool in the area of information security. It can provide data secrecy, integrity, usability and non-repudiation. It mainly consists of two parts, cryptography and cryptanalysis (Shen Changxiang et al. 2007). The top task of cryptography is to hide data using coding technology, while cryptanalysis is about obtaining the plaintext from cipher text. Figure 2.4 shows the conversion of plain text to cipher text using cryptography technique.
Figure 2.4 Conversion of plain text to cipher text (or) Encryption vs. Decryption

With the increasing popularity of biometrics, cryptography and a secret protection is driven by a common demand on information security. Biometric authentication is considered as one of the important secured system but biometric authentication itself follows some procedural algorithms like feature extraction, matching, classification etc. There is a possibility of intrusion at any step so it requires additional security management. Cryptography is one of the most effective method to enhance the security of the system (Sowkarthika and Radha 2012). The security level is based on the associated secret key. The simple memorized key can be easily intercepted, while the long and complex key requires extra storage management for tokens, smart cards etc. As a solution, secure encryption key can be associated with biometrics.

Here, some of the examples are given and briefly discussed about the cryptography technique, for both UBAS and MMBAS. Fingerprint and Public key cryptography (Okediran et al. 2011a), Iris with cryptography (Anderson et al. 2006), Error Correct Code (ECC) with Iris Key Generation (Xiangqian Wu et al, 2008), Voice and Signature with Hash function (Victor Morales-Rocha et al. 2008), Finger print and Signature with cryptography (Shweta Malhotra and Chander Kant Verma 2013)
Okediran et al., (2011a), proposed the requirement, design and implementation of a generic e-voting system using a number of electronic devices including private computer network, web and mobile phone. The security considerations of the model were based on RSA (Rivest-Shamir-Adleman) encryption algorithm for end to end message security and firewalls in the form of proxy server. The developed model provided ubiquitous voting service to electorate based on Public Key Cryptography (PKC) which offers high flexibility through end to end key agreement protocols and biometric fingerprint authentication mechanism. The model is an authoritative cryptographic model based on RSA with large key size which requires both large amount of computing time and consumes large storage size on both mobile and electronic voting device.

A realistic and secure way to incorporate the iris biometric into cryptographic applications was presented by Anderson et al. (2006). They deliberated on the error patterns within iris code and developed a two layered error correction code that merges Hadamard and the Reed Solomon code. The key was produced from the iris image of the subject through the auxiliary error correction data that do not disclose the key and can be saved in a tamper resistant token like smart card. These methodologies were evaluated with the help of samples from 70 different eyes, obtaining 10 samples for each eye. It was established that an error free key can be reproduced reliably from genuine iris code with a success rate of 99.5%. It is possible to produce up to 140 bits of biometric key, more than adequate for 128 bit Advanced Encryption Standard (AES). The Reed-Solomon (R-S) code is particularly useful for burst-error correction. Also, they can be used efficiently on channels where the set of input symbols is large. An interesting feature of the R-S code is that as many as two information symbols can be added to an R-S code of length n without reducing its minimum distance. This extended R-S code has a length of n + 2 and the same number of parity check symbols as the original code (Rashmi and Nag 2013).

Xiangqian Wu et. al. (2008) had developed a Novel Cryptosystem based on Iris Key Generation. This system proposes a novel biometric cryptosystem based on the most accurate biometric feature iris. In encryption phase, a quantified 256-
dimension textural feature vector (ie, a set of metrics calculated in image processing designed to quantify the perceived texture of an image) is firstly extracted from the pre-processed iris image using a set of 2-D Gabor filters. At the same time, an Error Correct Code (ECC) is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using Hash function. Some general encryption algorithms use this cipher key to encrypt the secret information. In decryption phase, a feature vector extracted from the input iris is firstly corrected using ECC. Then it is translated to the cipher key using the same Hash function. Finally, the corresponding general decryption algorithms use the key to decrypt the information and found that FAR is 0% and FRR is 5.5% for this system.

Victor Morales-Rocha et al. (2008) carried out a remote voter registration in a secure way. It protects from alterations in 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 techniques that do not require a public key infrastructure. It consists of creating a kind of biometric digital signature. That means a biometric characteristic that can give in the same time both authentication and integrity to the contents. Finally, they identified and proposed some biometric methods, such as handwriting and voice biometrics that can also bind the registration information to the voter identity. Combining this later feature with the use of cryptographic algorithms, such as hash functions, also provided a way to protect the integrity of voter registration information that can be suitable to implement in current environments.

Shweta Malhotra and Chander Kant Verma (2013) proposed a combined biometric system where one physical and one behavioral approach is used for identification or verification to uniquely identify a person. This approach takes two different biometric traits. One finger print as physiological and other online signature as behavioral biometric trait. Both are sensed by sensor, features are extracted by feature extractor modules, matcher module matches the traits with stored template, and each decision module decide the perfect matches. Finally decisions are combined in fusion unit using simple “AND” and decision is taken whether the individual is not an intruder.
b) **Steganography**

Steganography is an ancient art of hiding messages in a secret way that no one, apart from the sender and anticipated recipient, suspects the existence of the message. The advantage of steganography over cryptography, is that in steganography messages were hidden inside the image and do not attract attention of others to themselves whereas the encrypted data say the cipher text are plainly visible for the hacker which will stimulate suspicion. Since steganography is meant for the concealment of information it can be used to protect both messages and communicating parties whereas cryptography protects only the contents of a message. Here, for embedding the secret key in an image, the least-significant bit insertion method (Chandramouli and Memon 2001) is used. This is the simplest approach for hiding data within an image file where the binary representation of the hidden data is overwritten on to the Least Significant Bit (LSB) of each byte within the cover image.

LSB based technique is very popular for steganography in spatial domain. The simplest LSB technique replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. Using LSB technique, embed each pixel (8 bits) of the secret grey image in the corresponding pixel of the coloured cover image (24 bits) by doing the following (Linu Babu et al. 2013):

- Divide the pixel in the secret grey image into 2 groups of 3 bits and 1 group of 2 bits.
- Embed the resulted groups of bits in the corresponding pixel in the coloured cover image (embed the first group of 3 bits in the Red layer, the second group of 3 bits in the Green layer and the last group of 2 bits in the Blue layer)

Repeat the steps until you embed all the pixels of the secret image in the coloured cover image. Steganographic systems, can be divided into two categories,
one is in which the very existence of the message is kept secret, and non
Steganographic systems, in which the existence of the message need not be secret. Figure 2.5 shows the use of steganography for creating secret templates.

![Steganography diagram](image)

**Figure 2.5 Use of Steganography for creating secret template**

The hidden message is called the embedded message. A Steganographic algorithm combines the cover message with the embedded message, which is something to be hidden in the cover. The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded message again.

In many cases, the appropriate use of cryptography also reduces this threat (Chander Kant et al. 2005). The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric data before it is transmitted from one physical device to another. Steganography can greatly reduce these attacks because attackers must have to obtain the system’s private data in addition to breaching the security of the capture device or biometric storage. This makes these attacks considerably more difficult to achieve. But steganography is more secure than cryptography because there is no separate key (Figure 2.4) in steganography rather key is inbuilt in the template (Uludag et al. 2004).
Steganography can be used in a lot of useful applications. For example, in copyright control of materials, to enhance the robustness of an image search engine and smart identity cards where the details of individuals are embedded in their photographs. Other applications include video-audio synchronization, TV broadcasting, TCP/IP packets where a unique ID is embedded in an image to analyse the network traffic of particular users (Yunura Azura Yunus et al. 2013). Medical Imaging System is one of the modern applications that use Steganography where a separation is recommended between patient image data or DNA sequences and their captions for security or confidentiality reasons. Thus, embedding the patient information in the image could be a security measure to help solving security issues.

Here are some of the examples given and briefly discussed about the steganography technique, for both UBAS and MMBAS: Skin Detection Based Cryptography in Steganography (SDBCS) (Surendiran and Alagarsamy 2010), Finger print and Face authentication system using Steganography (Shanthini and Swamynathan 2012), Face and Voice recognition using Crypto-Stegano scheme (Alok Kumar Vishwakarma and Atul Kumar 2011).

Surendiran and Alagarsamy (2010) proposed a novel method in steganography using skin color detection scheme. This method introduced a two-way security mechanism in steganography using skin color detection scheme as well as cryptography. To ensure the strength of cryptography, Java Cryptography Architecture (JCA) is used. The proposed skin detection algorithms can detect skin regions accurately. Skin color has proven to be a useful and robust cue for face detection, localization and tracking. They have developed skipping and hybrid algorithm. Intuitiveness of the color space components and explicit discrimination between luminance and chrominance properties made these color spaces popular in the works on skin color segmentation The proposed method provided an application for Steganography using Color Space Transformations (CST) based on popular methods for skin color detection. Parametric skin modelling methods are better suited for constructing classifiers in case of limited training and expected target data set. The generalization and interpolation ability of these methods makes it possible to construct a classifier with acceptable performance from complete training data.
This method integrates the features of Cryptography and Color Space Transformation (CST) to provide the best of both worlds in information security.

Shanthini and Swamynathan (2012) proposed Multimodal Biometric-based Secured Authentication System using Steganography (MBSASS), with two biometrics say, fingerprint and face which are used to provide message security and user authentication. This system not only protects the message communicated between the users of high security applications of MANETs but also authenticates the sender in an implicit way. In this proposed model MBSASS, receiver’s fingerprint-based cryptographic key is used for encrypting the actual data and the key needs to be distributed among the users before the transaction takes place. Initially the fingerprint images of the users are acquired using fingerprint sensors and are pre-processed as explained in Shanthini and Swamynathan (2011a). The system proposed different pre-processing steps namely Normalization, Enhancement, Binarization, finding an orientation field map, finding a region of interest, thinning, removal of H breaks, removal of spikes and finally the features are extracted from the fingerprint image. Then spurious minutiae are removed from the extracted minutiae. At the same time the core point of the fingerprint image and the orientation field are also calculated.

Alok and Atul (2011), authors proposed a Crypto-Stegano scheme for mobile voting. The scheme is based on face and voice biometric recognition for authentication and ECC encryption for vote integrity and image steganography for confidentiality. The strength lies in the enhanced approach of ECC stego scheme to mobile voting platform.

c) **Scale Invariant Feature Transform (SIFT)**

This algorithm is the most widely used one for image feature extraction. Scale Invariant Feature Transform (SIFT) extracts image features, that are stable over image translation, rotation and scaling and somewhat invariant to changes in the illumination and camera viewpoint (David G. Lowe 2004). The SIFT algorithm has four major phases,
Extrema Detection – It examines the image under various scales and octaves to isolate points of the picture that are different from their surroundings. These points, called extrema, are potential candidates for image features.

Keypoint Localization – It starts with the extrema and selects some of these points to be keypoints, which are a set of feature candidates. This refinement rejects extrema that are caused by edges of the picture and by low contrast points.

Orientation Assignment – This converts each keypoint and its neighbourhood into a set of vectors by computing a magnitude and a direction for them. It also identifies other keypoints that may have been missed in the first two phases; this is done on the basis of a point having a significant magnitude without being an extremum. The algorithm now has identified a final set of keypoints.

Keypoint Descriptor Generation – It takes a collection of vectors in the neighbourhood of each keypoint and consolidates this information into a set of eight vectors called the descriptor. Each descriptor is converted into a feature by computing a normalized sum of these vectors.

One of the interesting features of the SIFT approach is the capability to capture the main grey level features of an object’s view by means of local patterns extracted from a scale-space decomposition of the image. In this respect, the SIFT approach is similar to the Local Binary Patterns (LBP) method (Zhang et al. 2004), with the difference of producing a view-invariant representation of the extracted 2D patterns.

Here are some of the examples given and briefly discussed about the Scale Invariant Feature Transform (SIFT) technique, for both UBAS and MMBAS: Detection of scale and affine transformations using SIFT (Krystian Mikolajczyk and Cordelia Schmid 2004), Finger-knuckle-print (FKP) based recognition system using SIFT and SURF (Adithya Nigam et al. 2011), SIFT based Face recognition (Yu-Yao
Wang et al. 2013), Face and Fingerprint recognition with Discrete Wavelet Transform (DWT) classifier (Bagal et al. 2013), Fusion of face and palm print using wavelet decomposition (Dakshina Ranjan Kisku et al. 2009), Multimodal biometric system using two biometric traits (Face and Palm Print) and three biometric traits (Face, Fingerprint and Palm Print) (Shekhar Karanwal 2013).

Krystian Mikolajczyk and Cordelia Schmid (2004), proposed a new approach for detecting interest points invariant to scale and affine transformations. The interest points extracted with the Harris detector can be adapted to affine transformations and give repeatable results (geometrically stable). The proposed scale invariant detector computes a multi-scale representation for the Harris interest point detector (David G. Lowe 2004) and then selects points at which a local measure (the Laplacian) is maximal over scales. This provides a set of distinctive points which are invariant to scaling, rotation and translation as well as robust to illumination changes and limited changes of viewpoint. The characteristic scale determines a scale invariant region for each point. Then it’s extended to the scale invariant detector to affine invariance by estimating the affine shape of a point neighbourhood. This method can deal with significant affine transformations including large scale changes.

Adithya Nigam et al. (2011) presented a novel combination of local-local information for an efficient Finger-Knuckle-Print (FKP) based recognition system which is robust to scale and rotation. The non-uniform brightness of the FKP due to relatively curvature surface is corrected and texture is enhanced. The local features of the enhanced FKP are extracted using Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF). Corresponding features of the enrolled and the query FKPs are matched using nearest-neighbour-ratio method and then the derived SIFT and SURF matching scores are fused using weighted sum rule. The proposed system is evaluated using PolyU FKP database of 7920 images for both identification mode and verification mode. It is observed that the system performs with CRR of 100% and EER of 0.215%. Further, it is evaluated against various scales and rotations of the query image and is found to be robust for query images downscaled up to 60% and for any orientation of query image.
Yu-Yao Wang et al. (2013) proposed a method for face recognition, which uses a coarse to fine strategy based on Scale Invariant Feature Transform (SIFT) feature. To recognize a test sample, this method chooses the N training samples with smaller distance as “candidates” set C, based on the Euclidian distance, and sort at the whole training samples in the ascending order. Then it counts the number of well-matched pairs of SIFT features between the test sample and each “candidate” in C, and sort the “candidate” samples in descending order. The proposed method combines a local feature with a holistic classification method. To optimize the data set and compute effectively, it chooses “candidate” twice based on Euclidian distance and SIFT features respectively, which reduce the computational complexity and enhance the effectiveness of face recognition at the same time. Besides anyone after picking out new “candidate” samples, use the whole samples in the same class as the new “candidate” rather only the new “candidate”. A number of experiments show that this method performs well on several face databases. The experiments based on Yale, YaleB, AR and ORL databases show that the proposed method outperformed other algorithms.

Bagal et al. (2013) proposed the combination of face and fingerprint recognition with Discrete Wavelet Transform (DWT) classifier. The database is collected for individuals by taking the image of 256x256 and resolution is set to 72 dpi. For the sake of the experiment cropped face has been taken which covers face only and for the fingerprint, cropped fingerprint has been taken which covers ridges and lines. Decomposition is done by DWT. After decomposition, image fusion is done by weighted averaging method, after obtaining the fused images of face and fingerprint, fused image is pre-processed by histogram equalization for normalization.

For facial and fingerprint image matching, SIFT feature comparison is done based on Euclidian distance of feature vectors for the recognition of human identity. Only the key point descriptor information is taken from image. But before this, fused image is normalized by histogram equalization, after invariant SIFT features are extracted from the fused image. For image matching and recognition, SIFT features are first extracted from a set of reference images and stored in a database.
Dakshina Ranjan Kisku et al. (2009) presents a novel biometric sensor generated evidence fusion of face and palm print images using wavelet decomposition for personnel identity verification. The approach of biometric image fusion at sensor level refers to a process that fuses multispectral images captured at different resolutions and by different biometric sensors to acquire richer and complementary information to produce a new fused image in spatially enhanced form. When the fused image is ready for further processing, SIFT operators are used for feature extraction and the recognition is performed by adjustable structural graph matching between a pair of fused images by searching the corresponding points using recursive descent tree traversal approach. The experimental result of this system provides 98.19% accuracy. It outperforms the other methods of unimodal face and palm print authentication with the recognition rates of 89.04% and 92.17%, respectively.

Shekhar Karanwal (2013) discusses about multimodal biometric system using two biometric traits (Face and Palm Print) and three biometric traits (Face, Fingerprint and Palm Print). The results from both systems are compared and it is proved that system with three traits is more secure and reliable as compared to the system with two traits. This concept can be generalized for a multimodal system with n biometric traits. Major emphasis in the work is given on wavelet decomposition of the images of the traits, fusion of the images and feature extractor algorithm SIFT. The proposed method for evidence fusion is presented which is based on the image decomposition into multiple channels depending on their local frequency. The wavelet transform provides a framework to decompose an image into a number of new images, each of them having a different degree of resolution. The wavelet based image fusion would be applied to two dimensional multispectral face, palmprint and fingerprint images. When the fused image is ready for further processing SIFT is used for feature extraction and matching is performed by unit vectors.

Table 2.1 shows the summary of literature review on UBAS and MMBAS, to enhance security in decision making along with their methodology used, contribution, strength and limitations:
<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>RESEARCH</th>
<th>METHOD</th>
<th>ADVANTAGES</th>
<th>LIMITATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Okediran et al. 2011(a)</td>
<td>RSA encryption algorithm</td>
<td>UBAS</td>
<td>High flexibility through end to end key agreement protocols</td>
<td>Computational cost is very high</td>
</tr>
<tr>
<td>Anderson et al. 2006</td>
<td>Two layered error correction codes (Hadamard and the Reed Solomon codes)</td>
<td>UBAS</td>
<td>Burst-error correction, where the set of input symbols is large</td>
<td>Time Consuming</td>
</tr>
<tr>
<td>Xiangqian Wu et al. 2008</td>
<td>Textural feature vector extracted using a set of 2-D Gabor filters</td>
<td>UBAS</td>
<td>Feature vector is translated to a cipher key using Hash function</td>
<td>Computational Overhead</td>
</tr>
<tr>
<td>Victor Morales-Rocha 2008</td>
<td>Content binding of Cryptography and Voice biometric</td>
<td>UBAS</td>
<td>Biometric digital signature is used</td>
<td>Not robust enough to determine an identity</td>
</tr>
<tr>
<td>Surendiran and Alagarsamy 2010</td>
<td>Integrates the features of Cryptography and Color Space Transformation (CST) to provide information security</td>
<td>UBAS</td>
<td>Java Cryptography Architecture (JCA) is used to detect skin regions accurately</td>
<td>Limited training data set is used</td>
</tr>
<tr>
<td>Shweta Malhotra and Chander Kant Verma 2013</td>
<td>Combination of finger print and online signature</td>
<td>MMBAS</td>
<td>Aim to increase the robustness of biometric system</td>
<td>Not an optimal one</td>
</tr>
<tr>
<td>Shanthini and Swamynathan 2012</td>
<td>Steganography using fingerprint and face to provide message security and user authentication</td>
<td>MMBAS</td>
<td>Spurious minutiae are removed from the extracted minutiae</td>
<td>Bad quality fingerprint and imposter attacks</td>
</tr>
<tr>
<td>REFERENCE</td>
<td>RESEARCH</td>
<td>METHOD</td>
<td>ADVANTAGES</td>
<td>LIMITATIONS</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alok and Atul 2011</td>
<td>Crypto-Stegano scheme for mobile voting based on face and voice biometric recognition</td>
<td>MMBAS</td>
<td>Enhanced approach of Error Correct Code (ECC) stego scheme to mobile voting platform</td>
<td>Initializing the parameters is a tedious task</td>
</tr>
<tr>
<td>Adithya Nigam et al. 2011</td>
<td>Finger Knuckle print with SIFT and SURF</td>
<td>UBAS</td>
<td>Low cost dedicated hardware</td>
<td>SURF consumes large storage space than SIFT</td>
</tr>
<tr>
<td>Yu-Yao Wang et al. 2013</td>
<td>Face recognition based on Scale Invariant Feature Transform (SIFT)</td>
<td>UBAS</td>
<td>Combines a local feature with a holistic classification method</td>
<td>Minimum pair distance gives the poorest results</td>
</tr>
<tr>
<td>Bagal et al. 2013</td>
<td>Face and Finger Print with DWT Classifier and SIFT</td>
<td>MMBAS</td>
<td>Decomposition image fusion is done by weighted averaging method and normalized by histogram equalization</td>
<td>Fingerprints are not suitable for non-collaborative individuals</td>
</tr>
<tr>
<td>Dakshina Ranjan Kisku 2009</td>
<td>Multisensor biometric system for multispectral images which captured at different resolutions</td>
<td>MMBAS</td>
<td>Acquire richer and complementary information to produce a new fused image in spatially enhanced form</td>
<td>Palm print is bigger in size. It needs more space to store the image</td>
</tr>
<tr>
<td>Shekhar Karanwal 2013</td>
<td>Two biometric traits (Face and Palm Print) and three biometric traits (Face, Fingerprint and Palm Print)</td>
<td>MMBAS</td>
<td>Feature extraction and matching is performed by unit vectors</td>
<td>Needs bigger storage space</td>
</tr>
</tbody>
</table>
2.4 CONCLUDING REMARKS

From the literature review, the secure biometric authentication methods related to the proposed research works have been analyzed and it is inferred that:

- Security of the cryptographic key is weak due to practical problems of remembering pass code. Since the pass code is not directly tied to a user, the system is unable to differentiate between the legitimate user and the attacker.

- In steganography LSB coding is not robust; the embedded information would be lost, because of resample of LSB coding. Robustness can be improved by using a redundancy technique while encoding the secret message. However, redundancy techniques reduce data transmission rate significantly.

- Scale Invariant Feature Transforms (SIFT) are well localized in both spatial and frequency domains, reducing the probability of disruption by occlusion, clutter, or noise. Large numbers of features can be extracted.

Several studies have demonstrated that by consolidating information from multiple sources, better performance can be achieved compared to the individual unimodal systems. Based on that, the research proposal in this work to combine face and finger knuckle print implemented using scale invariant feature transform (SIFT), provides lots of scope for biometric authentication system. Face recognition seems to be a good compromise between reliability and social acceptance and balances security and privacy well. It requires minimal user interface. Also in finger knuckle print the texture pattern is produced by the finger knuckle bending. It is highly unique and makes the surface a distinctive biometric identifier. Scale Invariant Feature Transforms (SIFT) are highly distinctive, which allows a single feature to be correctly matched with high probability against a large database of features, providing a basis for object and scene recognition. The cost of extracting these features is minimized. The issues in storage cost and computation cost involved in handling such a big feature descriptors were not addressed clearly in previous
works. The storage and computational costs are most important things of typical authentication system which will decide the portability of the biometrics system. This work address the issues related with storage and computational costs involved in SIFT based face and finger knuckle print authentication system. No other combination of face and finger knuckle print authentication system using SIFT was proposed so far. This motivated the researcher to focus on Multimodal Biometric Authentication System (MMBAS) using SIFT and the remaining chapters of this thesis will explain the implementation, results and discussions on MMBAS.