A TWO LAYER IMAGE AUTHENTICATION & ENCRYPTION SCHEME THROUGH ECC & VOICE FEATURES (MFCC, PITCH VALUE)

Thesis Submitted in Partial Fulfillment of the Requirements for the Award of the degree of

Master of Technology
IN
INFORMATION SYSTEM

SUBMITTED BY

VIKAS PARDESI
(2K11/ISY/21)

UNDER THE GUIDANCE OF

N. S. RAGHAVA
ASSOCIATE PROFESSOR

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI-110042
(2011-2013)

CERTIFICATE

This is to certify that Mr. **VIKAS PARDESI (2K11/ISY/21)** has carried out the major project titled **" A Two Layer Image Authentication & Encryption Scheme through ECC & Voice Features (MFCC, Pitch Value)"** as a partial requirement for the award of **Master of Technology** degree in **Information System** by **Delhi Technological University, Delhi.**

The Major project is a bonafide piece work carried out and completed under my supervision and guidance during the academic session 2011-2013. The Matter contained in this report has not been submitted elsewhere for the award of any other degree.

Date:

(Project Guide)
N.S. Raghava
Associate Professor
Department of Information Technology
Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I express my gratitude to my major project guide **Mr. N.S.Raghava**, **Associate Professor** in **Information technology** Department at **Delhi Technological University, Delhi** for the valuable support and guidance he provided in making this major project. It is my pleasure to record my sincere thanks to my respected guide for his constructive criticism and insight without which the project would not have shaped as it has.

I humbly extend my word of gratitude to other faculty members of this department for providing their valuable help and time whenever it was required.

VIKAS PARDESI

Roll No.: 2K11/ISY/21

M.Tech (Information System)

Department of Information Technology

Delhi Technological University, Delhi

ABSTRACT

Speech Processing is an area in which we can find such unique features (Mel Frequency Cepstrum Coefficients, Pitch value, zero crossing rates etc.) in voice segment for recognition of any individual and pre-processing for further synthesis. In this paper we are presenting a simplified approach to image authentication with MFCC (Mel Frequency Cepstrum Coefficients) and Pitch Value and image Encryption through Elliptic Curve Cryptography. Because of ECC great advantages (small key size, no solution to discrete logarithmic problem, less time consuming encryption, infinite time taken for brute force attack) for handheld, portable devices. Applying MFCC and Pitch information with various methods on various encrypted images which is encrypted by Elliptic Curve Cryptography and at the receiver side we do reverse process of this approach for authentication and decryption of image .With this approach we can authenticate an image through voice segment which is advantageous because speech is a natural way to interact with people, Not required to sit and work with a keyboard and finally no specific training is required for end users.

Image processing is a branch of Computer Science in which we study about images and its processing for further additional improvements in the images. When we apply speech details in the image then our image get distracted and forms a new image and then we transfer it in the network by this we can do two types of work in the image processing area first one is we can authenticate an image and second one is encryption of the image because when we receive the image on receiver side then we can apply the same voice on image and apply reverse operation and can find the same image and after decryption of image we get the original image. In speech processing area there are such features of voice as pitch frequency and fundamental frequency and MFCC coefficients and many other features that are unique. On this basis we can use these features to process out in any field with other one in detail.

Applications and usage of this proposed system is to make our data transferring more authenticated and encrypted through latest technology i.e. elliptic curve cryptography. Now days secure data transmission is the main challenge of our priority. In this proposed system we are just providing the external schema of the authentication and encryption detail .we are not considering any kind of complexity comes under the authentication protocols.

Due to this proposed system we can make our system and data more secure and added another step to security of the data in the network.

LIST OF FIGURES

TABLE OF CONTENTS

Chapter 1

INTRODUCTION TO CRYPTOGRAPHY

1.1 Cryptography

Cryptography is the work and study of techniques for infrastructure of secure communication in the presence of third parties or hackers (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography [1] include ATM cards, computer passwords, and electronic commerce.

Cryptography was earlier to the new age was effectively working with cryptographic encryption, the conversion of data from a known state to apparent nonsense. The developer of an cryptic message shared the coding-decoding technique needed to recover the real information only with real/intended recipients, thereby concluding undesired persons to do the same. Now Since the World-War I and the starting of the computer, the ways that are used to carry out cryptography have become increasing rapidly and its application more widely used.

Latest cryptography [1][7] is very much depends on mathematical theory and computer science/information technology practice; basic cryptographic algorithms are implemented/designed around computational hardness assumptions, becoming such algorithms very difficult to break by any adversary. It is only theoretically possible to break such kind a system but it is impossible to do so by any known practical means. These methods are therefore called computationally very much secure; theoretical advances, for example improvements in basic integer factorization methods, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that this cannot be broken and also with unlimited basic computing power for an example is the one-time pad method but these procedures are hard to using this than the best results are breakable but computationally very much secure mechanisms.

Classical Cryptography

The older forms of writing secret information required little greater than pen and paper, as most persons could not understand. More literacy, or literate opponents, required actual cryptography. The most known classical cipher are transposition ciphers, which shuffle the order of letters in an information (e.g., 'what are you doing' becomes 'tahw ear you gniod' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically change words or groups of words with other words or groups of words (e.g., 'hello world' becomes 'jdhgs jsjdu' by replacing each letter with the one precede it in the Latin alphabet). Simple updating of any have never provided any confidentiality from enterprising opponents. An old substitution cipher was the Caesar cipher, in which each word in the plaintext was changed by a word some fixed no. of positions further below the alphabet. Suetonius realize that Julius Caesar done it with a shift of three positions to communicate with his seniors. Abash is an example of an old Hebrew cipher. The previous known use of cryptography is some cipher text on stone in Egypt, but this may has been create for the entertainment of literate observers instead than as a way of concealing message. Cryptography is done in the Kama Sutra as a process for lovers to interact with each other without inconvenient discovery.

The Greeks of ancient times are said to have known of ciphertext (e.g., the scytale transposition cipher claimed to have been implemented by the Spartan military in the classical times). Steganography (i.e., hiding the presence of information so as to make it secret) was also first discovered in classical times. A previous times example, from Herodotus, concealed a information—a picture on a slave's unshaved head—below the grown hair. Another Greek method was developed by Polybius (now called the "Polybius Square"). More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

Cipher texts produced by a classical cipher (and some latest ciphers) always conceal important data or information about the plaintext, which can mostly be used to track them. After the development of frequency analysis perhaps by the Arab mathematician and polymath, Al-

Kind (also known as *Alkindus*), in the 9th century, nearly all such ciphers became higher or lower readily stolen by every informed crypt attacker. Those classical ciphers are still enjoying popularity nowadays, though mostly as puzzles (see cryptogram). Al-Kindi wrote a book on cryptography entitled *Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*), which described the first cryptanalysis techniques.

Modern Cryptography-

The latest field of cryptography can be classified into various areas. The most known ones are explained here;

1.2 Cryptographic Attacks

An ATTACK can take place on any of the communications link.

For an **active attack**, the cryptanalyst needs to have physical control of a portion of the message and be able to update and capture transmissions of message (medium could be telephone twisted pair, coaxial cable, or optical fiber).
For a **passive attack**, the cryptanalyst merely needs to be able to view transmissions only (may be inductive taps).

1.2.1 Active attack: is an attack which the attacked person knows of when attack is being done. That is the intervention from the cryptanalyst is of such kind that he/she knows about the attack, so it is called active attacks. For example, trying to hack some information or important data.

1.2.2 Passive Attack: when the attacked entity does not know about the attack, so it is called passive attacks. For example, the attacker is only trying to observe or view your information.

1.3 Types of Cryptography

Generally there are two types of cryptography algorithm-

1.3.1 Symmetric-key cryptography

It refers to encryption techniques in which both the transmitter and receiver share the same cryptography key (or, more commonly, in which their keys are not same, but related in an different computable process). This was the only known type of encryption publicly understandable until June 1976. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are blocking cipher designs which have been designated cryptography standards by the US embassy (though DES's method was totally finished when the AES was started to be in use). Despite its ending as an official way, DES (formally its still-approved and much higher secured triple-DES variation) is still quite known and famous; it is implemented across a wide variety of applications, from ATM cryptography to e-mail security and secret remote access. Many different block ciphers have been developed and used, with variation in quality and procedure. Many have been thoroughly wasteful, such as FEAL.

Stream ciphers, in respect to the 'block' type, develop an arbitrarily long combination of key material, which is streamed with the known text bit-by-bit or character-by-character, like the one-time pad. In the stream cipher, the resulted stream is developed based on a hidden internal structure which exchange as the cipher does. That internal structure is firstly set up using the secret cryptographic key material. RC4 is a widely used stream cipher; see Category: Stream ciphers. Block ciphers can be used as stream ciphers; see Block cipher modes of operation as shown in figure (1.1).

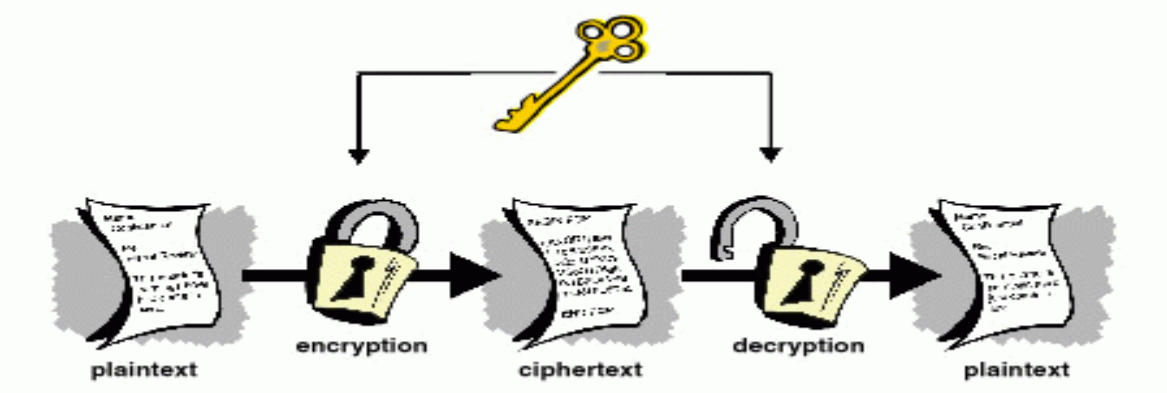

Fig-1.1 Symmetric Key Cryptography

Cryptographic hash functions are another type of cryptographic algorithm. They intake a message of any measure as input, and provide a little, static length hash which can be further used in (for example) a digital signature. For better hash functions, it should be difficult for an attacker that cannot find two messages which generate the same hash. MD4 is a widely used hash function which is now broken by an attacker; MD5 is a variant of MD4, is also mostly used but broken in general. The U.S. National Security Agency discovered the Secure Hash Algorithm variants of MD5-like hash functions: SHA-0 was a useless algorithm that the agency withdrew after sometime; SHA-1 is widely used and much more secured than MD5, but it is also broken by some cryptanalysts; the SHA-2 family provide some changes on SHA-1, but it is not still widely used, and the U.S. standards authority understand it "prudent" from a security point of view to create a new standard to "efficiently improve the robustness by having some changes of NIST's overall hash algorithm toolkit." Thus, a hash function design competition was developing to create a new U.S. national standard, which is to be called SHA-3, by 2012. The competition ended on October 2, 2012 when the NIST announced that Keycap would be the new SHA-3 hash algorithm. Message authentication codes are much more like cryptographic hash functions, other than that a cryptographic secret key can be implement to authenticate the hash value after received.

1.3.1.1 Caesar Cipher Algorithm-s

In cryptography, a **Caesar cipher**, also known as **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the easiest and most widely known encryption techniques. It is a type of substitution cipher in which each word in the plaintext is changed by a word some static no. of positions below the alphabet. For example, with a left shift of 3, D would be replaced by A; E would become B, and so on. The method is named after Julius Caesar, who discovered it in his private correspondence.

The encryption procedure performed by a Caesar cipher is widely incorporated as part of more difficult schemes, such as the Vigenere cipher, and still has modern application in the ROT13 system. As with all one alphabet substitution ciphers, the Caesar cipher is very easily

broken by cryptanalysts and in latest practice provides essentially no interaction security services.

The transformation can be presented by two different alphabets; the cipher alphabet is the known alphabet shifted right or left by some no. of positions. For instance, here we provide a Caesar cipher by using a left shift of 3 places, equivalent to a right rotation of twenty three (the rotation parameter is used as the key):

```
2   Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
3   Cipher:   XYZABCDEFGHIJKLMNOPQRSTUVW
```

When encrypting, people saw each word of the information in the "plain" line and keep down the simultaneous word in the "cipher" line. Decryption is done in reverse of encryption, with a right shift of 3.

```
4   Cipher text: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
5   Plaintext:  the quick brown fox jumps over the lazy dog
```

1.3.1.2 Data Encryption Standard (DES)

The **Data Encryption Standard [18]** is a previously predominant algorithm for the encryption of e-data. It was more influential in the development of latest cryptography in the world of academics. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's proposal to propose a candidature for the security of sensitive, classified electronic government information. In 1976, after consulting with the National Security Agency (NSA), the NBS eventually selected a slightly updated variant, which was developed as an official Federal Information Processing Standard (FIPS) for the US in 1977. The publication of an NSA-approved encryption technique standard corresponds resulted in its quick international adoption taken and widespread academic scrutiny. Controversies arose out/in of design materials, a relatively big key length of the symmetric-key block cipher design of cryptography, and the great involvement of the NSA, nourishing suspicions about a backdoor.

The intense academic scrutiny the algorithm retained over time led to the latest understanding of block ciphers and their corresponding cryptanalysis.

DES is now related to be not secure for many widely used applications. This is mainly because of the 56-bit key length being too small; in Jan, 1999, distributed.net and the Electronic Frontier Foundation collaborated to break a DES cryptographic key in 21 hours and 55 minutes (see chronology). There are also some theoretical results which demonstrate analytical weaknesses in the ciphertext, although they are impossible to mount in general. The algorithm is believed to be practically secured in the way of Triple DES, although there are analytical attacks. In previous years, the cipher has been considered by the Advanced Encryption Standard (AES). Furthermore, DES has been backed up as a procedure by the National Institute of Standards and Technology (formerly the National Bureau of Standards).

Some analysis makes a difference between DES as a standard and DES as an algorithm, provided to the algorithm as the **DEA** (**Data Encryption Algorithm**) as shown in figure (1.2, 1.3, 1.4).

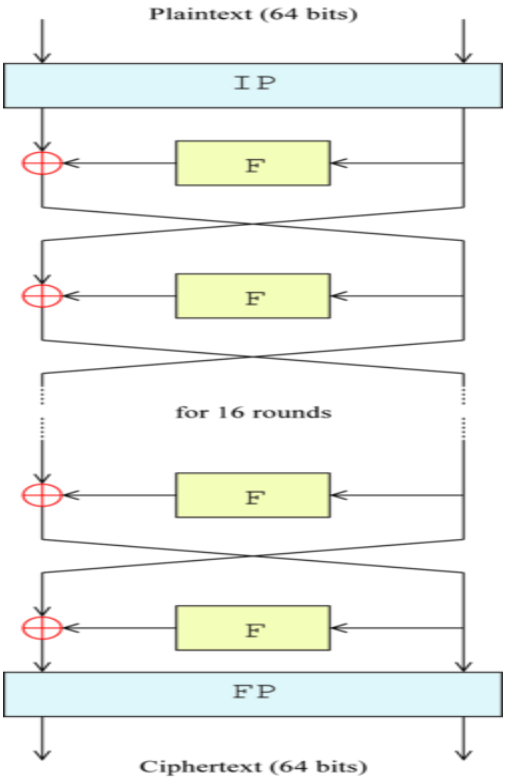

Fig-1.2 the overall Feistel structure of DES

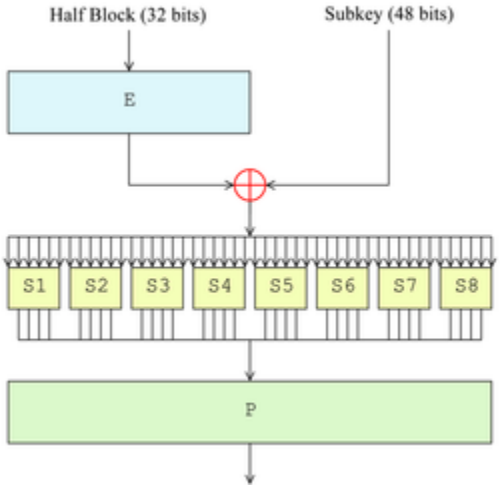

Fig-1.3 the Feistel function (f function of DES)

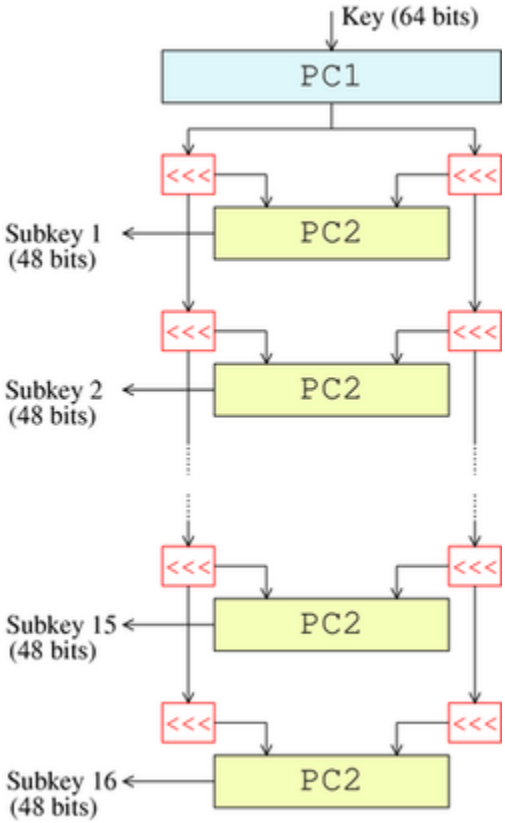

Fig-1.4 the key schedule of DES

1.3.1.3 Advanced Encryption Standard

The **Advanced Encryption Standard** (**AES**) is a specification for the encryption of electronic data generated by the U.S.National Institute of Standards and Technology (NIST) in 2001.It is based on the **Rijndael** cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who provided a proposal which was consulted by the NIST in the period when AES process is selected.

AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1976. The algorithm evaluated by AES is a symmetric-key algorithm, means the same cryptographic key is evaluated for both encryption and decryption of the message.

In the United States, AES was published by the NIST as U.S. FIPS PIB 198 (FIPS 197) on November 27, 2002. This announcement succeed for more than four-year standardization process where fifteen competing designs were represented and considered, before the Rijndael cipher was announced as the most efficient (see Advanced Encryption Standard procedure for extra information). It became popular as a federal government standard on May 27, 2002 after appropriate by the Secretary of Commerce. AES is inserted in the ISO/IEC 18033-4 standard. AES is provided in many different encryption techniques, and is the most publicly accessible and open cipher succeeded by the National Security Agency (NSA) for most secret message when implemented in an NSA approved cryptographic standard.

The name *Rijndael* is a play on the names of the two inventors (Joan Daemen and Vincent Rijmen). Strictly speaking, the AES standard is a variant of Rijndael where the block size is restricted to 128 bits.

1.3.2 Asymmetric Key Cryptography

Symmetric-key cryptography uses the identical key for encryption and decryption of information, though information or group of information may have a different key than any others. An efficient disadvantage of symmetric ciphers is the key management necessary to use them secretly. Each same pair of interacting parties must, ideally, share a same key, and perhaps

each cipher text shared as well. The no. of keys necessary increases as the square of the no. of network members increased, which very quickly needs simple key management procedure to keep them all straight and secured. The weakness of securely establishing a secured key between two interacting parties, when a secret channel does not exist between them, also represents a chicken-and-egg problem which is a considerable general obstacle for cryptography users in the world. In a groundbreaking 1976 paper, David Kahn and Martin Hellman developed the procedure of *public-key* (also, more practically, called *asymmetric key [19]*) cryptography in which two non-identical but mathematically related keys are implemented—a *public* key and a *private* key. A public key procedure is so constructed that evaluation of one key (the 'secret key') is computationally impossible from the other (the 'public key'), even though they are necessarily related. Despite, both keys are created securely, as an interrelated pair. The historian David Kahn considered public-key cryptography system as "the most revolutionary new system in the field since polyalphabetic substitution emerged in the Renaissance".

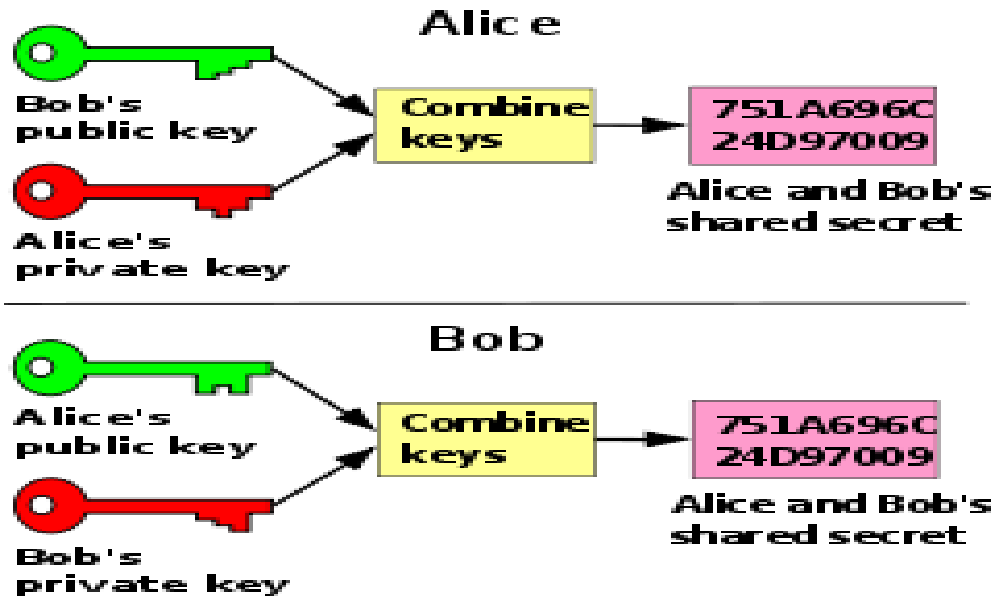

Fig-1.5 an Example of Public key Cryptography

As shown in figure (1.5) in public-key cryptography, the public key may be freely shared, while its paired private cryptography key must remain secured. In a public-key encryption system, the *public key* is used for encryption, while the *private* or *secret key* is used for decryption. While Diffie and Hellman could not find such a system, they showed that public-key cryptography was

indeed possible by presenting the Diffie–Hellman key exchange protocol, a solution that is now widely used in secure communications to allow two parties to secretly agree on a shared encryption key. Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adelman, whose solution has since become known as the RSA algorithm.

The RSA and Diffie–Hellman algorithms, in addition to being the most publicly known examples of higher popular public-key algorithms, being among the most suitably used. Others include the Cramer–Shoup cryptosystem, ElGamal encryption, and various elliptic curve techniques. See Category: Asymmetric-key cryptosystems.

Too much surprise, a document published in 1997 by the Government Communications Headquarters (GCHQ), a British intelligence organization, revealed that cryptographers at GCHQ had anticipated several academic developments. Reportedly, around 1970, James H. Ellis had conceived the principles of asymmetric key cryptography. In 1973, Clifford Cocks invented a solution that essentially resembles the RSA algorithm. And in 1974, Malcolm J. Williamson is claimed to have developed the Diffie-Hellman key exchange.

1.3.2.1 RSA System

The RSA [20] algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters **RSA** are the initials of their surnames, listed in the same order as on the paper.

MIT was granted U.S. Patent 4,405,829 for a "Cryptographic communications system and method" that used the algorithm in 1983. The patent would have expired on September 21, 2000 (the term of patent was 17 years at the time), but the algorithm was released to the public domain by RSA Security on September 6, 2000, two weeks earlier. Since a paper describing the algorithm had been published in August 1977, prior to the December 1977 filing date of the patent application, regulations in much of the rest of the world precluded patents elsewhere and only the US patent was granted. Had Cocks' work been publicly known, a patent in the US might not have been possible, either.

From the DWPI's abstract of the patent, the system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to cipher text at the encoding terminal by encoding the message as a number M in a predetermined set. That number is then raised to a first predetermined power (associated with the intended receiver) and finally computed. The remainder or residue, C, is... computed when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver).

Clifford Cocks, an English mathematician working for the UK intelligence agency GCHQ, described an equivalent system in an internal document in 1973, but given the relatively expensive computers needed to implement it at the time, it was mostly considered a curiosity and, as far as is publicly known, was never deployed. His discovery, however, was not revealed until 1998 due to its top-secret classification, and Rivest, Shamir, and Adleman devised RSA independently of Cocks' work.

Key Generation

RSA involves a **public key** and a **private key.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
    - For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a Primality test.
2. Compute $n = p\,q$.
    - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.

4. Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are co-prime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
5. Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

   - This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm.
   - d is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The **public key** consists of the modulus n and the public (or encryption) exponent e. The **private key** consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.
- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits *c* to Alice.

Decryption

Alice can recover *m* from *c* by using her private key exponent *d* via computing

$$m \equiv c^d \pmod{n}.$$

Given *m*, she can recover the original message *M* by reversing the padding scheme.

(In practice, there are more efficient methods of calculating c^d using the pre computed values below.)

1.3.2.2 Elliptic Curve Cryptography

Public-key cryptography is based on the intractability of certain mathematical solutions. Early public-key procedures are protected assuming that it is hard to factor a small integer composed of three or more huge prime factors. For elliptic-curve-based procedures, it is considered that discovering the discrete logarithm of a simultaneous elliptic curve element with need to a publicly aware base point is inflexible. The length of the elliptic curve discovered the hardness of the solution. The most benefit consulted by ECC [2][10][11] is a higher key size, inserting storage and communication requirements—i.e., that an elliptic curve group could stand the different level of privacy provided by an DES-based system with a huge modulus and correspondingly greater length key—e.g., a 264-bit ECC public key should provide comparable security to a 3084-bit DES public key (see *key sizes* below).

For current cryptographic purposes, an *elliptic curve* is a plane curve which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b,$$

Along with a distinguished point at infinity, denoted ∞. (The coordinates described here are to be selected from a fixed finite field of characteristic not equal to 3 or 4, or the curve formula will be somewhat highly complex.)

This set together with the group operation of the elliptic group theory form an Abelian group, with the point at indefinite as normal element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

As for other known public key cryptosystems, no mathematical evidence of privacy has been published for ECC as of 2008. However, the U.S. National Security Agency has endorsed ECC by inserting procedures based on it in its Suite C set of considered procedures and permits their use for providing information classified up to top private with 390-bit keys. While the RSA patent ends in 2001, there are some patents in force covered some aspects of ECC technology, though most (including RSA Laboratories and Daniel J. Bernstein) suggested that the Federal elliptic curve digital signature standard (ECDSD; NIST FIPS 187-4) and mostly practical ECC-based key transformed schemes (including ECDH) can be implemented without infringing them.

1.4 Cryptanalysis

Cryptanalysis is the method of obtaining the meaning of encrypted information without the information of the secret parameters that are normally required to obtain the meaning. This typically involves the knowing of the system, how it works and discovered the private key. In non-technical procedure, this is the solution of data breaking or cracking the code, although these phrases have a specialized technical meaning. "Cryptanalysis" is used also to protect to any try to circumvent the privacy of some other kinds of cryptographic procedures and protocols in practical and not just encrypt the message. However, cryptanalysis usually left out the methods of attack that do primarily target hardness in the real and private cryptography, although these kinds of attack are an most important and highly concern and are often more efficient than ealier cryptanalysis. The International Telecommunication union-Telecommunication standardization Sector (ITU-T) provides some security services and some mechanism to implement those services.

Chosen plain text attack

A **chosen-plaintext attack** (**CPA**) is an attack model for cryptanalysis which presumes that the cryptanalyst has the ability to select arbitrary plaintexts to be encrypted and obtain the

corresponding cipher texts. The primary motive of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key. For some chosen-plaintext attacks, only a small part of the plaintext needs to be chosen by the attacker: such attacks are known as **plaintext injection** attacks.

Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and cipher text-only attacks; this is a conservative approach to security.

Two forms of chosen-plaintext attack can be distinguished:

Chosen cipher text attack

A **chosen-cipher text attack** (**CCA**) is an attack model for cryptanalysis in which the attack collects all the information, at least in part, by selecting a cipher text and gaining its decryption under an unknown key. In the attack, an adversary has an option to insert one or more known cipher texts into the algorithm and access the final plaintexts. From this breakdown code of information the adversary can try to rediscover the hidden private key implemented for decryption process.

A no. of otherwise secure procedures can be defeated under selected cipher text attack. For example, the ElGamal cryptosystem is semantically secure under selected plaintext attack, but this semantic privacy can be defeated under a selected cipher text attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-cipher text attack which revealed SSL session keys. Chosen-cipher text attacks have implications for some self-synchronizing stream ciphers as well.

When a cryptosystem is vulnerable to selected cipher text attack, implementers must be take precautions to avoid the problems in which an adversary may be able to decrypt selected cipher texts (i.e., deselect by providing a decryption oracle). This can be much harder than it looks, as even fully selected cipher texts can admit subtle attacks. Furthermore, some cryptosystems procedures (such as RSA) use the same algorithm to sign messages and to transform in

unreadable form. These types of attacks when hashing is not used on the message to be signed. A good approach is to have a cryptosystem which is provably protect under selected cipher text attack, including (among others) RSA-OAEP, Cramer-Shoup and many forms of authenticated symmetric encryption.

Known plain text attack

The **known-plaintext attack (KPA)** is an attack model for cryptanalysis where the attacker has samples of both the plaintext (called a **crib**), and its encrypted version (cipher text). These can be used to reveal further secret information such as secret keys and code books. The term "crib" originated at Bletchley Park, the British World War II decryption operation

Man in the Middle Attack

The **man-in-the-middle attack** (often abbreviated **MITM**, **MitM**, **MIM**, **MiM**, **MITMA**, also known as a **bucket brigade attack**, or sometimes **Janus attack**) in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle).

This maneuver precedes computers. A fictional example of a "man-in-the-middle attack" utilizing a telegraph is featured in the 1898 short story The Man Who Ran Europe by Frank L. Pollack.

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other — it is an attack on mutual authentication (or lack thereof). Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, SSL can authenticate one or both parties using a mutually trusted certification authority.

1.5 Security Services

The security services include:

- Data Confidentiality
- Data Integrity
- Authentication
- Non repudiation
- Access Control

Data Confidentiality

Confidentiality has been defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography. It is designed to protect data from disclosure attack. The service as defined by X.800 is very broad and encompasses confidentiality of whole message or part of a message and also protection against traffic analysis. That is it is designed to prevent snooping and traffic analysis.

Data Integrity

Data Integrity is designed for the protection of data from unauthorized modification, insertion, deletion and replaying by an advisory. It can protect the whole message or the part of message.

Authentication

This service provides the authentication of the party at the other end of the line. In the connection oriented communication, it provides the authentication of the sender or receiver during the connection establishment (peer entity authentication). In connectionless communication, it authenticates the source of data (also called data origin authentication).

Non-repudiation

Non-repudiation service protects against repudiation by either the sender or the receiver of the data. In this with the proof of origin, the receiver of the data can later prove the identity of the sender. If denied, in non-repudiation with the real proof of delivery the sender of the data can later prove the data were delivered to the intended recipient. Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refuse the validity of a statement or contract. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

Access Control

Access control now it is a system that can enable a body/system to control the access to major areas and such resources in given detailed virtual information or computer architecture-based basic information system. An access control system, within the field of basic layer security, is generally can be seen as the second layer approach in the security of a basic layer structure. It provides security against unauthorized access against data. The term access in this definition is very broad and can involve reading, writing, modifying, executing programs.

An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure. It provides security against unauthorized access against data. The term access in this definition is very broad and can involve reading, writing, modifying, executing programs.

1.6 Cryptographic Background

1.6.1 Random Number Generation

A random number generator is a computational physical device is getting generated a sequence of numbers is being attacked that can be any pattern, i.e. appear random. The very much large scale of applications of probability is being led to the development of several different methods for creating random data. Many of those is being existed since the last ancient modern times; including dice, coin flipping, and the shuffling of playing cards, the use of yarrow stalks (by divination) in the I Chin, and many other techniques. Because of the mechanical nature of these techniques, generating large amounts of sufficiently random numbers (important in statistics) required a lot of work and/or time.

They are used in cryptography so long as the seed is secret. Sender and receiver can generate the same set of numbers automatically to use as keys.

Random Number Generation plays a vital role in Group Signatures. A basic property of any Group Signature is that it should be untraceable and Random Number Generators help satisfy the property. Each time a member signs a message; randomness in the algorithm ensures that the signatures are different from each other and that no outsider can reveal the identity of the signer from the signature, neither can he claim that two signatures are signed by the same member. Random Number Generators also help reduce the burden of assigning values to parameters required to setup the group.

1.6.2 Primality Test

Primality test is an basic desired steps for determining it is an input number is prime or not. From all other fields of branch mathematics, it is being used for cryptography. Unlike integer method of factorization, basic Primality tests do not share generally give prime numbers and factors, only stating that whether the given input number is prime or not. As of 2010, factorization is a computationally difficult problem, whereas now it is said that Primality testing is easy in comparison with the. Some Primality tests can prove that a it is a number is not prime,

while others like basic algorithm Miller-Rabin is proving that a number is being composite or not. Therefore we might call the latter compositeness tests instead of Primality tests.

Primality tests come in two varieties: deterministic and probabilistic.

Deterministic Algorithm: A deterministic Primality testing algorithm accepts an integer and always outputs a prime or a composite. Deterministic basic tests will determine with the absolute certainty number that is on the whether a number is prime. Until recently, all deterministic algorithms were so insufficient at finding larger primes that they were considered infeasible. In 2002, Agrawal, Kayal and Saxena announced that they had found an algorithm for Primality testing with polynomial time complexity of O ($(\log^{12} n)$).

Probabilistic Algorithm: Probabilistic results can be potentially (although such a very large probability) not truly identifying a real number as not prime (although vice versa). However, they are so much general very much slower than deterministic tests. digitaly that has been passed a very much probabilistic integer test are therefore properly being referred to as a probable primes approach until the Primality test can be illustrated deterministically.

Fermat's Test: The first probabilistic, method is discussed in the Fermat Primality test:

If n is a prime, then $a^{n-1} \equiv 1 \pmod{n}$

Note that this means if n is prime, the congruence holds. It does not mean that if the congruence holds, n is prime. The integer can be prime or composite. It can define the following as Fermat's test:

If n is a prime, then $a^{n-1} \equiv 1 \bmod n$

If n is composite, it is possible that $a^{n-1} \equiv 1 \bmod n$

All primes pass the Fermat's test. Composite may also pass the Fermat's test as well. The bit operation complexity of Fermat's test is same as the complexity of an algorithm that calculates the exponentiation.

Square Root Test: In modular arithmetic, if n is a prime the square root of 1 is either +1 or -1. If n is composite the square root is +1 or -1, but there may be other roots. This is known as square root Primality test.

If n is a prime, sqrt (1) mod n=+1 or -1

If n is a composite, sqrt (1) mod n=+1 or -1 and possibly other values.

Miller-Rabin Primality Test: The Miller-Rabin Primality test combines the Fermat's test and square root test in a very elegant and efficient way to find a strong pseudo prime (a prime with a very high probability of being a prime). In this test write n-1 as the product of an odd number and a power of two.

$n-1 = m* 2^k$

In other words, instead of calculating a^{n-1} (mod n) in one step, it can do it in k+1 steps. The benefit is that in each step, the square root test can be performed. If the square root test fails it is stop and declare that n is a composite number. In each step it is assure ourselves that the Fermat's test is passed and the square root test is satisfied between all pairs of adjacent steps, if applicable. It is a probabilistic method. There exists a proof that each time the number passes the Miller-Rabin Primality Test, the probability that it is not a prime is 1/4. If the number passes m tests (with m different bases) the probability that it is not a prime is $(1/4)^m$.

1.6.3 Discrete Logarithm

In mathematical background, generally in algebra and it's mostly applications, discrete logarithms [7] are group analogues of specially logarithms. In general, and specifically logarithm $\log_a$ (b) is a result of the equation $a^x = b$ over the actual or highly complex numbers. Same, if r and s are elements of a definite cyclic group T then a result x of the equation $r^x = s$ is called a discrete logarithm to the base r of s in the group T.

In general, let T be a definite cyclic group with m terms. It is considered that the group is basically multiplicatively. Suppose w be a generator of T; so every element r of T can be written in the form $r = w^k$ for various integer k. Additional, any 2 such integer's g1 and g2 corresponds to r must be congruent modulo m. We can thus finally provide a function

$\log_b: T \rightarrow Z_m$

Where Zm represents the ring of integers modulo m by providing to each r the congruence group of k modulo m. This defined function is a group isomorphism, which is called the discrete logarithm to base b.

The known base change formula for particular logarithms remains still valid: If d is another generator of T, so

$\text{Log}_d(r) = \log_d(b) * \log_b(r)$

No effective earlier algorithm for conducting general discrete logarithms $\log_b r$ is aware. The naive procedure is to raise b to lower and lower powers k up to the considered r is known; this is generally called trial multiplication. This procedure needs waiting time linear in the length of the group T and so exponential in the no. of digits in the length of the group. There exists an effective quantum procedure due to David Shor.

More commutated procedure exists, usually viewed by similar procedure for integer factorization. These procedures run greater and efficient than the naive procedures, but no one runs in lesser time (in the no. of digits in the length of the group).

1.6.4 Integer Factorization

In no. theory system, prime factorization or decimal factorization is the division down of a composite no. into small non-trivial divisors, which when divide together results the previous original integer.

When the no. is very huge, no effective integer factorization procedure is unknown; an effort concerned in 2010 by several analyst of this field factored a 234-digit no. (RSA-766) utilizing thousands of machines over a span of 2 and half years. The presumed disadvantage of this procedure is at the heart of certain procedure in cryptography such as DES. Many fields of mathematics system and computer science (cryptography and network security) have been brought to bear on the solution, excluding elliptic curves, number theory, and quantum computing procedure.

All no. of a presumed size are equally difficult to factor. The difficult instances of these procedures (for currently aware solutions) are semi primes, the multiply of two non-prime no. When they are both huge, chosen as random, and about the different length (but not too far away), even the highest prime factorization procedures on the highest computers can take more time to create the search impossible.

1.7 Application & Advantages of Cryptography

Cryptography, for most of the people, is related with having communications secret. In fact, the security of sensitive transmissions has been the concentration of cryptography throughout much of its in previous and recent times. Encryption is the process in which data is transformed into some unpredictable form. Its motive is to ensure secrecy by keeping the communications hidden from everyone for whom it is not supposed to be, even those who can view the transformed data. Decryption is the process inverse of encryption; it is the method in which encrypted data is transformed back into some readable form.

Encryption and decryption need the implementation of some private information, usually known as a key. Depending on the encryption procedure analyzed, the same key can be used for encryption and decryption process, while for other procedure; there should be different key for encryption and decryption process.

In cryptography and network security, an adversary's solution is a calculation of how easily it can attack a cryptographic problem, by differentiating it from an idealized method of that type of procedure. It is to be noted that in this context, the "adversary" is referred to an algorithm and not anyone. A cryptographic procedure is known secured if no adversary has a negligible disadvantage, consulted to specified bounds on the adversary's mathematical resources (see concrete security). "Negligible" usually means "within $\underline{O}(2^{-p})$" where p is a security parameter associated with the algorithm. For example, p might be the no. of bits in a block cipher's key.

Chapter 2

ELLIPTIC CURVE CRYPTOGRAPHY

2.1 What is Elliptic Curve Cryptography (ECC)?

Elliptical Curve Cryptography (ECC) [2][10][11] is an another way of implementing public-key cryptography(creates a mechanism for exchanging keys among huge numbers of candidates or entities in a complex information management system). ECC is different from other popular algorithms such as RSA, based on discrete logarithms that are very much difficult to tackle at same key lengths. At the time of its invention, the ECC algorithm was told and placed in the public interest. Certicom focused its efforts after found that it provided higher potential secured way it was slow by creating worst implementations of the procedure to improve its performance. After a long time of research, Certicom presented the first commercial toolkit to support ECC that make it possible for use in various applications. Other cryptographer is taking interest in ECC. Today Certicom sponsors the Centre for Advanced Cryptographic Research (CACR) at the Waterloo University. Every year, they sponsor an ECC workshop which is attended by over 100 top cryptographers to discuss advancement in the area of elliptical curve cryptography. Other more important industry activity is receiving additional credibility to the technology. The Certicom ECC Challenge offers an opportunity those for those public around this world to form a new way of attack the rules and exposing any weaknesses. The higher an algorithm resides up to the attack the more you have the confidence manufacturers have in its ultimate security applications. The EC Cryptography Challenges commenced in November 2000 and still running today. company hosts an annual Certicom authority EC Cryptography Conference, which takes almost together thinkers leaders, researchers and industry persons to talking about EC Cryptography and its applications and uses. Also important is the recreation of the Standards for Efficient Cryptography Group. The basic SECG is a committee of leading basic providers of cryptography and detailed information security methods and algorithms solutions who have united to address of interoperability by today's different different cryptographic solutions. Asymmetric cryptography is a marvelous technology. Its uses are many and varied. And then you indeed needed it, you need it. For many situations in infrastructure of distributed network

environments, asymmetric key cryptography is a basic communication during communications. If you're having key distribution causes with a public key distributions infrastructure (PKI), you're using asymmetric key cryptography. If you're designing or employing any kind of networking rules or protocols or application basic needs secure communications and infrastructures, to come up with the leading practical solutions, you're going to have to use asymmetric cryptography. Asymmetric cryptography having, in fact, providing so useful for securing talking that it has become pervasive in real practical life. Every time you buy something over the Internet, if the vendor is maintaining a secure socket server, you were using asymmetric key cryptography scheme to securing the transaction details. But asymmetric key cryptography is demanding and really complex structure, by its very much nature. The core detail hard problems in number and group theory — the key to the step wise procedure functionality — are all intrinsically difficult enough that the processor repetition cycles you must throw at doing it, and/or the chip space you have to dedicate to the real time implementation, unavoidable far outstripping the resources you hve done you must dedicated for doing symmetric cryptography. So, if you need asymmetric cryptography, you should choose a kind that uses the least resources. Elliptic curve cryptography (ECC) is the best choice, because:

• ECC offers very much detail version of considerably greater security for a given length key size.

• The lesser key guard size also making finite much more complicated implementations for a given increasing level of security, which means slower cryptographic operations, running on smaller integrated chips or complex much more compact software. it means less heat production and very much less power consumption by the circuit — all of which are particular advantage in restrained devices, but of very some advantage anywhere.

• There are highly effective, comprises hardware implementation provided for ECC exponentiation resolutions operations, offering potential strengthen reducing in implementation foot-print even more beyond those due to the lesser key length alone.

In short: asymmetric cryptography is very much in demand in market. But if you're searching for the system which is for cryptography that will give you the most security per bit,

you want ECC. This paper describes elliptic curve cryptography technology in greater depth — how it is working, and why it offers many of these advantages. It will start by discussing the large subject of asymmetric key cryptography in general. ECC is offering considerably greater security for a given key size.

Why Asymmetric Cryptography?

ECC is a method of a set of algorithms for key generation, encryption and decryption to doing asymmetric cryptography [19]. Asymmetric cryptographic algorithms have the property that you do not use a single key as in symmetric cryptographic algorithms good such as secure AES but a key pair. One of basic of the the keys (the public key) was used for encryption, and its corresponding real private key must be used for decryption. The very much critical feature of asymmetric key cryptography, that is used to make it very much useful, is this A-key pair and more complex specifically, a particular represented feature of the nice key pair: the fact that one of the asymmetric keys could not be get from the other one. Authentication With normal Asymmetric key Cryptography normally In the case of asymmetric key authentication methods the core power technology behind basic digital signatures and digital certificates it is normally said of a private key (in the real owenment of the entity having to prove its uniqueness) and the public key infrastructure (in the real possession of anyone who wishes to verify the identity of the entity possessing the private key).You may, real world with the public key, verify that an entity has been acknowledge of the private key but you could not derive the private key derivation from the public key technology. This is the basic critical feature of asymmetric cryptographic procedure that makes there is so useful. These properties are useful for a number of things: it greatly simplified public-private key exchange, as one example, and it solves one critical problem symmetric cryptography cannot result the problem of sure unique authentication and non-repudiation familiar. Symmetric key hashing/authentication methods ones for which there is only remaining one key, and both parties in the transferring use it both for authentication and for basic digital signature generation have the distinct disadvantage that they do not, on their own, offer any way to want to distinguish which party of the transferring signed a given message. If both or all parties much know the key algorithms infrastructures, based on cryptography alone, you cannot distinguish which signed any given message, because any of

them could have. In asymmetric authentication schemes, only one party knows the private key, with which the message is signed. many number would know the public key algorithm. Since the private key could not be derived from the public key derivation, the signature then serves as a unique representation identifier. If the message being verifies as having been digitally signed by the real person with knowledge of the infrastructure of the private key, this can narrow down the message who sent the message to one another. But many number of people may will have knowledge of the infrastructure of the public key, and all of them can therefore verify the identity of the sender details. If you're looking for the cryptosystem that will give you the most security per bit, you want ECC.

Use of each of the public-key cryptographic schemes described in this document involves arithmetic operations on an elliptic curve over a finite field. This section introduces the mathematical concepts necessary to understand and implement these arithmetic operations.

.

Elliptic Curves

An elliptic curve over [2][10][11] q is defined in terms of the solutions to an equation in q. The form of the equation defining an elliptic curve over q differs depending on whether the field is a prime finite field or a characteristic 2 finite field as shown in figure (2.1).

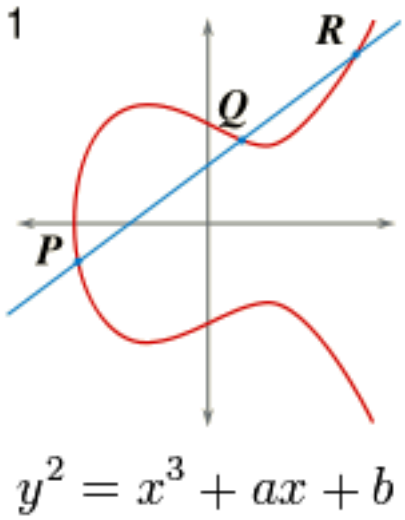

Fig- 2.1 an Elliptic Curve

The set of points on E p forms a group under this addition rule. Furthermore the group is abelian - meaning that P1 P2 P2 P1 for all points P1 P2 E p . Notice that the addition rule can always be computed efficiently using simple field arithmetic.

Cryptographic schemes based on ECC rely on scalar multiplication of elliptic curve points. Given an integer k and a point P E p , scalar multiplication is the process of adding P to itself k times. The result of this scalar multiplication is denoted k P or kP. Scalar multiplication of elliptic curve points can be computed efficiently using the addition rule together with the double-and-add algorithm or one of its variants.

2.1.1 Group Theory

In mathematics, a **group** is a set of elements together with an operation that combines any two of its elements to form a third element also in the set while satisfying four conditions called the group axioms, namely closure, associativity, identity and invertibility. One of the most familiar examples of a group is the set of integers together with the addition operation; the addition of any two integers forms another integer. The real version of abstraction formulations of the group axioms details, detached as it is from the discrete nature of any real group and its operation being involved, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.

Groups share a fundamental kinship with the notion of symmetry. For example, a symmetry group encodes symmetry features of a geometrical object: the group consists of the set of transformations that leave the object unchanged, and the operation of combining two such transformations by performing one after the other. Lie groups are the symmetry groups used in the Standard Model of particle physics; Point groups are used to help understand symmetry phenomena in molecular chemistry; and Poincaré groups can express the physical symmetry underlying special relativity.

The concept of a group arose from the study of polynomial equations, starting with Évariste Galois in the 1830s. After contributions from other fields such as number

theory and geometry, the group notion was generalized and firmly established around 1870. Modern group theory—a very active mathematical discipline—studies groups in their own right. To explore groups, mathematicians have devised various notions to break groups into smaller, better-understandable pieces, such as subgroups, quotient groups and simple groups. In addition to their abstract properties, group theorists also study the different ways in which a group can be expressed concretely (its group representations), both from a theoretical and a computational point of view. A particularly rich theory has been developed for finite groups, which culminated with the monumental classification of finite simple groups announced in 1983. Since the mid-1980s, geometric group theory, which studies finitely generated groups as geometric objects, has become a particularly active area in group theory.

Definition-

A group is a set, G, together with an operation • (called the *group law* of G) that combines any two elements a and b to form another element, denoted $a \bullet b$ or ab. To qualify as a group, the set and operation, (G, •), must satisfy four requirements known as the *group axioms*:

Closure

For all a, b in G, the result of the operation, $a \bullet b$, is also in G.

Associativity

For all a, b and c in G, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

Identity element

There exists an element e in G, such that for every element a in G, the equation $e \bullet a = a \bullet e = a$ holds. Such an element is unique and thus one speaks of *the* identity element.

Inverse element

For each a in G, there exists an element b in G such that $a \bullet b = b \bullet a = e$.

The result of an operation may depend on the order of the operands. In other words, the result of combining element a with element b need not yield the same result as combining element b with element a; the equation

$$a \bullet b = b \bullet a$$

May not always be true. This equation always holds in the group of integers under addition, because $a + b = b + a$ for any two integers (commutativity of addition). Groups for which the commutativity equation $a \bullet b = b \bullet a$ always holds are called *abelian groups* (in honor of Niels Abel). The symmetry group described in the following section is an example of a group that is not abelian.

The identity element of a group G is often written as 1 or 1_G, a notation inherited from the multiplicative identity. The identity element may also be written as 0, especially if the group operation is denoted by +, in which case the group is called an additive group. The identity element can also be written as *id*.

The set G is called the *underlying set* of the group $(G, \bullet)$. Often the group's underlying set G is used as a short name for the group $(G, \bullet)$. Along the same lines, shorthand expressions such as "a subset of the group G" or "an element of group G" are used when what is actually meant is "a subset of the underlying set G of the group $(G, \bullet)$" or "an element of the underlying set G of the group $(G, \bullet)$". Usually, it is clear from the context whether a symbol like G refers to a group or to an underlying set.

2.1.2 ECC on Binary Field

On binary field it only means that it work upon these equations Binary: GF(2^m)

$Y^2 + XY = X^3 + aX^2 + b$ with $b \neq 0$

An "elliptic curve" means points on the curve plus the point at infinity.

2.1.3 ECC on Finite Field

Abstractly a finite field consists of a finite set of objects called field elements together with the description of two operations - addition and multiplication - that can be performed on pairs of field elements. These operations must possess certain properties. It turns out that there is a finite field containing q field elements if and only if q is a power of a prime number, and furthermore that in fact for each such q there is precisely one finite field. The finite field containing q elements is denoted by q.

Here only two types of finite fields q are used — finite fields p with q p, p an odd prime which are called prime finite fields, and finite fields 2m with q 2m for some m 1 which are called characteristic 2 finite fields. It is necessary to describe these fields concretely in

order to precisely specify cryptographic schemes based on ECC.it describes prime finite fields and Section 2.1.2 describes characteristic 2 finite fields

2.1.4 ECC over Real numbers

The finite field p is the prime finite field containing p elements. Although there is only one prime finite field p for each odd prime p, there are many different ways to represent the elements of p. Here the elements of p should be represented by the set of integers:
Addition and multiplication in p can be calculated efficiently using standard algorithms for ordinary integer arithmetic. In this representation of p, the additive identity or zero element is the integer 0, and the multiplicative identity is the integer 1.

It is convenient to define subtraction and division of field elements just as it is convenient to define subtraction and division of integers. To do so, the additive inverse (or negative) and multiplicative inverse of a field element must be described:

2.2 Operations Involved in ECC Encryption

2.2.1 Point Addition

Point addition is defined as taking two points along a curve *E* and computing where a line through them intersects the curve. Use the negative of the intersection point as the result of the addition.

The operation is denoted by $P + Q = R$, or $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$. This can algebraically be calculated by:

$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$
$$x_r = \lambda^2 - a - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$

Where *a* is the multiplication factor of x^2 in the elliptic field. Note that often, *a* will be zero, reducing complexity of the equation as shown in figure (2.2).

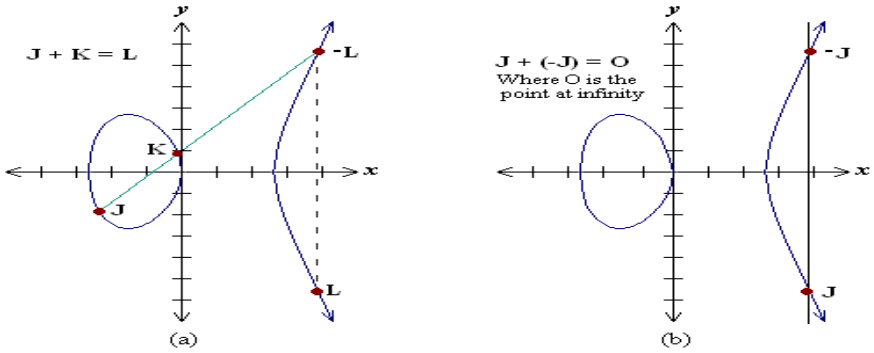

Fig-2.2 Point Addition

2.2.2 Point doubling

Point doubling is similar to point addition, except take the tangent of a single point and find the intersection with the tangent line.

$$\lambda = \frac{3x_p^2 + 2ax_p + b}{2y_p}$$

$$x_r = \lambda^2 - a - 2x_p$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Note that only λ has changed with respect to the point addition problem. Note that it is assume that the elliptic field is given by $x^3 + ax^2 + bx + c$. as shown in figure (2.3).

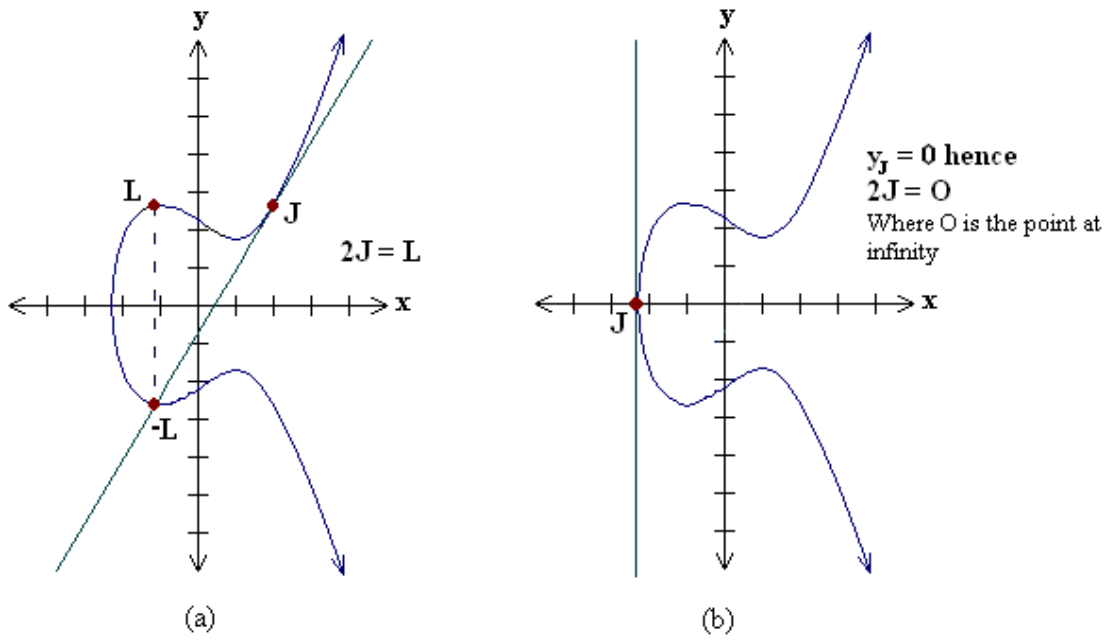

Fig-2.3 Point Doubling

2.2.3 Point Multiplication

Elliptic curve point multiplication is the operation of successively adding a point along an elliptic curve to itself repeatedly. It is used in elliptic curve cryptography (ECC) as a means of producing a trapdoor function. The literature presents this operation as scalar multiplication, thus the most common name is "Elliptic curve scalar multiplication", as written in Hessian form of an elliptic curve.

Given a curve ξ defined along some equation in a finite field (such as $y^2 = x^3 + ax^2 + bx + c$) define point multiplication as the repeated addition of a point along that curve. Denote as $nP = P + P + P + ... + P$ for some scalar (integer) n and a point $P = (x, y)$ that lies on the curve.

The security of modern ECC depends on the intractability of determining n from $Q = nP$ given known values of Q and P. It is known as the elliptic curve discrete logarithm problem.

2.3 Operations involved in ECC decryption

2.3.1 Discrete Logarithmic Problem

In mathematics, specifically in abstract algebra and its applications, **discrete logarithms** are group-theoretic analogues of ordinary logarithms. In particular, a simple logarithm $\log_a(b)$ is a solution of the equation $a^x = b$ over the real or complex numbers. Similarly, if g and h are elements of a finite cyclic group G then a solution x of the equation $g^x = h$ is called a discrete logarithm to the base g of h in the group G

Discrete logarithms is very much perhaps simply to understand in the group $(\mathbf{Z}_p)$. This is the set $\{1, \ldots, p-1\}$ of congruence classes under multiplication modulo the prime p.

If we want to find the kth power of one of the numbers in this group, it can do so by finding its kth term power is as an-integer and then find the remainder after division by p. This process is called *discrete exponentiation*. For example, consider $(\mathbf{Z}_{17})$. To compute 3^4 in this group, first compute $3^4 = 81$, and then divide 81 by 17, obtaining a remainder of 13. Thus $3^4 = 13$ in the group.

Discrete Logarithmic is just the just inverse operation. For example, take the equation $3^k \equiv 13 \pmod{17}$ is for k. As below shown is above above k=4 is not a solution, but it is not the only solution. Since $3^{16} \equiv 1 \pmod{17}$ — which is know from little theorem of fermats— it also follows that the following if n was an integer then $3^{4+16n} \equiv 3^4 \times (3^{16})^n \equiv 13 \times 1^n \equiv 13 \pmod{17}$. Hence the equation has infinitely many solutions of the form $4 + 16n$. Moreover, since 16 is the smallest positive integer m satisfying $3^m \equiv 1 \pmod{17}$, i.e. 16 is the order of 3 in $(\mathbf{Z}_{17})^\times$, here it is the only 1 solutions. alternatively, the solution may be expressed as $k \equiv 4 \pmod{16}$.

In general, let G be a finite cyclic group with n elements. It is assume that the group is written multiplicatively. Let b be a generator of G; then every element g of G can be written in the form $g = b^k$ for some integer k. Furthermore, any two such integers k_1 and k_2 representing g will be congruent modulo n. this can thus define a function

$$\log_b : G \to \mathbb{Z}_n$$

(Where $\mathbf{Z}_n$ denotes the ring of integers modulo n) by assigning to each g the congruence class of k modulo n. This function is a group isomorphism, called the discrete logarithm to base b.

The regular base changing formula for simple logarithms remains valid: If c is another generator of G, then

$$\log_c(g) = \log_c(b) \cdot \log_b(g).$$

ALGORITHMS

No effective classical algorithm for calculating general discrete logarithm problem $\log_b g$ is known as follows. The naive algorithm is to raise b to higher and higher powers k until the desired g is found; this is sometimes called *trial multiplication*. This algorithm requires running time linear in the size of the group G and so main thing is exponential number in the in the number of digital digits in the size of the main group. There exists one basic effective quantum algorithm due to Peter Shor.

Very much ultra-sensual algorithms exist, usually made by similar algorithms for integer factorization. These algorithms run very much fast than the naive algorithm, but none of them runs in default runtime polynomial time (in the number of digits in the whole size of the group).

- Baby-step giant-step
- Pollard's rho algorithm for logarithms
- Pollard's kangaroo algorithm (aka Pollard's lambda algorithm)
- Pohlig–Hellman algorithm
- Index calculus algorithm
- Number field sieve
- Function field sieve

Comparison with Integer factorization

While the trouble of calculating discrete logarithmic and the problem of integer factorization are distinct problems they will share some extra properties:

- both problems are difficult the very much basic view (no efficient algorithms are known for non-quantum computers),
- for both problems efficient algorithms on quantum computers are known,
- algorithms from one problem are often adapted to the other, and
- The difficulty of both problems has been used to construct various cryptographic systems.

In future ECC is going to be in demand because it has great advantage over other public cryptography scheme such as RSA and DES. In RSA and DES the main problem is key size and more over head for computation of Permutation and combination.

2.4 Advantages/ Disadvantages

a) Key size and Digital Signature that are generated through ECC are very shorter in size compare to other cryptographic scheme.

b) This is based on discrete logarithmic form so easily can be converted into elliptic curve form.

c) No time consumes for permutation and combination and less time taking for encryption.

d) Till date no solution found for breaking the Discrete Logarithmic approach so brute force attack on ECC takes too many years (uncountable).

e) Very much suitable for handheld devices such as palm top mobile phones PDA because they are low memory devices and ECC can work better on this.

Disadvantages-

a) ECC uses curves generators fields' etc. This is more complex to calculate so this is not good for processor health.

b) ECC systems are much slower than RSA in large no. of public key generation.

c) For calculating more complex variables so it is also not good for device's resources such as memory, processor etc.

2.5 Applications of Elliptic Curve Cryptography

a) Simple Key generation by ECC is a great application in cryptography.

b) Shorter Certificate

c) Shorter Signature can also be generated with the help of ECC.

Generally till date ECC worked only in constrained environment such as less memory shorter devices and limited ROM and limited processing speed so it may be our new future work to make ECC more independent from system and devices and constrained environment.

Now move to the IPV6 because there are some drawbacks in IPV4 such as when transfer our data then IPSEC protocol and IPV4 can't work simultaneously and it has to be improved for better working and secure transmission of the data and elliptic curve cryptography is the solution for this because when transfer the data by the RSA (Rivest-Shamir-Adleman) algorithm then its key size is very long and data can be corrupted in middle of the way but elliptic curve cryptography contains very small key compare to RSA and when it is transfer the data through ECC then corruption of data has less chances so do more work in this field.

Chapter 3
SPEECH PROCESSING

3.1 Introduction

Speech processing [3][4] is the study of speech signals and the interpretation methods of the signals. The digital signals are normally processed in a digital representation, so digital speech processing can be explained as a very special case of digital signal processing, applied to speech signal. Aspects of speech processing include the acquiring, manipulation/modification, storage, transfer and output of digital speech signals.

It is also closely tied to natural language processing (NLP), as input will come from / output/input can go to NLP applications. E.g. text-to-speech synthesis may use a syntactic parser on its input text and speech recognition's output may be used by e.g. information extraction techniques. The main applications of speech processing are the recognition, synthesis and compression of human Speech sounds are sensations of air and noise pressure basic vibrations is being produced by air simulated exhaled from the lungs and modulated and demodulated shaped by the vibrations of the real sense of glottal cords and the resonance of the vocal tract is as per the air is pushed out through-out the lips and nose.

Speech is an immensely information-rich signal exploiting frequency-modulated, amplitude-modulated and time-modulated carriers (e.g. resonance movements, harmonics and noise, pitch intonation, power, duration) to convey information about words, speaker identity, accent, expression, style of speech, emotion and the state of health of the speaker. All this information is conveyed primarily within the traditional telephone bandwidth of 4 kHz. The speech energy above 4 kHz mostly conveys audio quality and sensation.

In this chapter the fundamentals of speech signals and speech production and perception are studied. It is study the mechanisms that produce and convey phonetic speech sounds and examine the acoustic correlates of speaker characteristics such as gender, accent and emotion. The spectral and temporal structures of speech are studied and the most commonly used models and features for capturing speech characteristics in time and frequency are introduced. Speech coding methods for improving bandwidth utilization and power efficiency in

mobile communication are covered. Finally, study automatic speech recognition for a simple voice- dialing application. Speech is an immensely information-rich signal exploiting frequency-modulated, amplitude-modulated and time-modulated carriers (e.g. resonance movements, harmonics and noise, pitch intonation, power, duration) to convey information about words, speaker identity, accent, expression, style of speech, emotion and the state of health of the speaker. All this information is conveyed primarily within the traditional telephone bandwidth of 4 kHz. The speech energy above 4 kHz mostly conveys audio quality and sensation.

In this chapter the fundamentals of speech signals and speech production and perception are studied. It is studied the mechanisms that produce and convey phonetic speech sounds and examine the acoustic correlates of speaker characteristics such as gender, accent and emotion. The spectral and temporal structures of speech are studied and the most commonly used models and features for capturing speech characteristics in time and frequency are introduced. Speech coding methods for improving bandwidth utilization and power efficiency in mobile communication are covered. Finally, study automatic speech recognition for a simple voice- dialing application. While you are producing speech sounds, the air flow from your lungs first passes the glottis and then your throat and mouth. Depending on which speech sound you articulate, the speech signal can be excited in three possible ways:

• Voiced excitation the glottis is closed. The air pressure forces the glottis to open and close periodically thus generating a periodic pulse train (triangle–shaped). This "fundamental frequency" usually lies in the range from 80Hz to 350Hz.

• Unvoiced excitation the glottis is open and the air passes a narrow passage in the throat or mouth. This results in a turbulence which generates a noise signal. The spectral shape of the noise is determined by the location of the narrowness.

• Transient excitation, A closure in the throat or mouth will raise the air pressure. By suddenly opening the closure the air pressure drops down immediately. ("plosive burst")

With some speech sounds these three kinds of excitation occur in combination. The spectral shape of the speech signal is determined by the shape of the vocal tract (the pipe formed by your throat, tongue, teeth and lips). By changing the shape of the pipe (and in addition opening and closing the air flow through your nose) you change the spectral

shape of the speech signal, thus articulating different speech sounds.

Technical Characteristics of the Speech Signal

An engineer watching at (or listening audio to) a digital speech signal might classifieds it as follows:

• The bandwidth of the digital signal is 3.9 kHz. The signal is periodic in motion with a basic fundamental frequency between 82 Hz and 352 Hz

• There are some peaks in the digital spectral distribution of energy at

$$(2*n-1)*500\,Hz\,;\ n=1,2,3,\ldots \qquad (1.1)$$

• The envelope due to of the power spectrum of the digital signal showing a decrease with increasing frequency.

This is a very random rough and technical/specific description of the digital speech signal. But where do those characteristics come from?

Bandwidth

The bandwidth and idea of the digital speech signal is very much higher than the 3.9 kHz stated shown above. In fact, for the fricatives, there is still a significant amount of energy in the spectrum for high and even ultrasonic frequencies. However, as all know from using the phone, it seems that with-in a bandwidth of 3.9 kHz the digital speech signal contains all the information essential to understand a human voice/speech.

3.1.1 Fundamental Frequency

As described earlier, using voiced excitation for the speech sound will result in a pulse train, the so-called fundamental frequency. Voiced excitation is used when articulating vowels and some of the consonants. For fricatives (e.g., /f/ as in fish or /s/, as in mess), unvoiced excitation (noise) is used. In these cases, usually no fundamental frequency can be detected. On the other hand, the zero crossing rate of the signal is very high. Plosives (like /p/ as in put), which use transient excitation, you can best detect in the speech signal by looking for the short silence necessary to build up the air pressure before the plosive bursts out.

Peaks in the Spectrum

After passing the glottis, the vocal tract gives a characteristic spectral shape to the speech signal. If one simplifies the vocal tract to a straight pipe (the length is about 17cm), one can see that the pipe shows resonance at the frequencies as given by (1.1). These frequencies are called formant frequencies. Depending on the shape of the vocal tract (the diameter of the pipe changes along the pipe), the frequency of the formants (especially of the 1st and 2nd formant) change and therefore characterize the semi-vowel being changed.

The Envelope of digital Power Spectrum Decreasing with Increment in Frequency

The pulse digital sequence from the glottiana has a power digital spectrum decrement towards higher frequencies by -11dB/octave. The extraction characteristics of the lips shown a high-pass specific characteristic with +6.2dB per octave.

Speech Communication

Speech is the most natural form of human communication. Speech is one of the most information-laid signals; speech sounds have a rich and multi-layered temporal-spectral variation that convey words, intention, expression, intonation, accent, speaker identity, gender, age, style of speaking, state of health of the speaker and emotion.

Speech sounds are produced by air pressure vibrations generated by pushing inhaled air from the lungs through the vibrating vocal cords and vocal tract and out from the lips and nose airways. The air is modulated and shaped by the vibrations of the glottal cords, the resonance of the vocal tract and nasal cavities, the position of the tongue and the openings and closings of the mouth.

Just as the written form of a language is a sequence of elementary alphabet, speech is also a sequence of elementary acoustic sounds or symbols known as phonemes that convey the spoken form of a language. There are about 40-60 phonemes in the English language from which a very large number of spoken words can be constructed. Note that in practice the production of each phonemic sound is affected by the context of the neighboring phonemes.

Speech signals convey much more than spoken words. The information conveyed by speech is multi-layered and includes time- frequency modulation of such carriers of information as formants and pitch intonation. Formants are the resonances of vocal tract and pitch is the sensation of the fundamental frequency of the opening and closings of the glottal folds. The information conveyed in speech includes the followings:

(a) Acoustic phonetic symbols. These are the most elementary speech units from which larger speech units such as syllables and words are formed. Some words have only two phones such as 'me', 'you', 'he'.

(b) Prosody. These are rhythms of speech mostly intonation signals carried by changes in the pitch trajectory and stress. Prosody help to signal such information as the boundaries between segments of speech, link sub-phrases and clarify intention and remove ambiguities such as whether a spoken sentence is a statement or a question.

(c) Gender information. Gender is conveyed by the pitch (related to the fundamental frequency of voiced sounds) and the size and physical characteristics of the vocal tract. Due to differences in vocal anatomy, female voice has higher resonance frequencies and a higher pitch.

(d) Age, conveyed by the effects of the size and the elasticity of the vocal cords and vocal tract, and the pitch. The pitch of voice o children can be more than 300 Hz.

(e) Accent, broadly conveyed through: (i) changes in the pronunciation dictionary in the form of substitution, deletion or insertion of phoneme units in the "standard" transcription of words (e.g. Australian *tod**ie*** pronunciation of *tod**ay*** or US *J**aa**n* pronunciation of *J**o**hn*) and (ii) systematic changes in speech resonance frequencies (formants), pitch intonation, duration, emphasis and stress.

(f) Speaker's identity conveyed by the physical characteristics of a person's vocal folds, vocal tract, pitch intonations and stylistics.

(g) Emotion and health, conveyed by changes in: vibrations of vocal fold, vocal tract resonance, duration and stress and by the dynamics of pitch and vocal tract spectrum.

In the remainder of this chapter it will be study how various acoustic correlates of speech and speaker can be modeled and used for speech processing applications.

3.1.2 Acoustic Theory of Speech [8][5]: The Source-Filter Model

An outline of the anatomy of the human speech production system is shown. It consists of the lungs, larynx, vocal tract cavity, nasal cavity, teeth, lips, and the connecting tubes. The combined voice production mechanism produces the variety of vibrations and spectral-temporal compositions that form different speech as shown in figure (3.1).

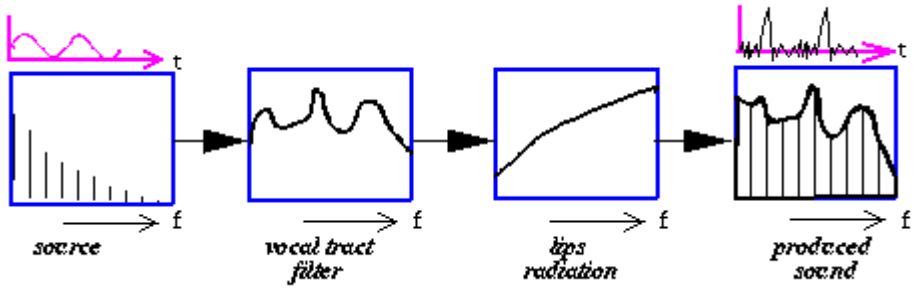

Fig-3.1 the Source Filter Model of Human Speech Production

The act of production of speech begins with exhaling (inhaled) air from the lung. Without the subsequent modulations, this air will sound like a random noise with no information. The information is first modulated onto the passing air by the manner and the frequency of closing and opening of the glottal folds. The output of the glottal fold is the excitation signal to the vocal tract which is further shaped by the resonances of the vocal tract and the effects of the nasal cavities and the teeth and lips.

The vocal tract is combined with hard and soft tissue tough structures. These structures is either necessarily im-mobile, such as the very much hard palate and teeth or movable objects. The mobile structured associated speech productions are also known *articulators*. The tongue, side lips, side jaw, and velum are the basic articulators; movement and positioning of these articulators appears to responsible/account for most of the capabilities in the vocal tract shaping associated with speaking person. However, another structures are capable of motion as well. For instance, the glottiana can be vary up or down to decreasing or lengthen the vocal tract and so change its frequency result response.

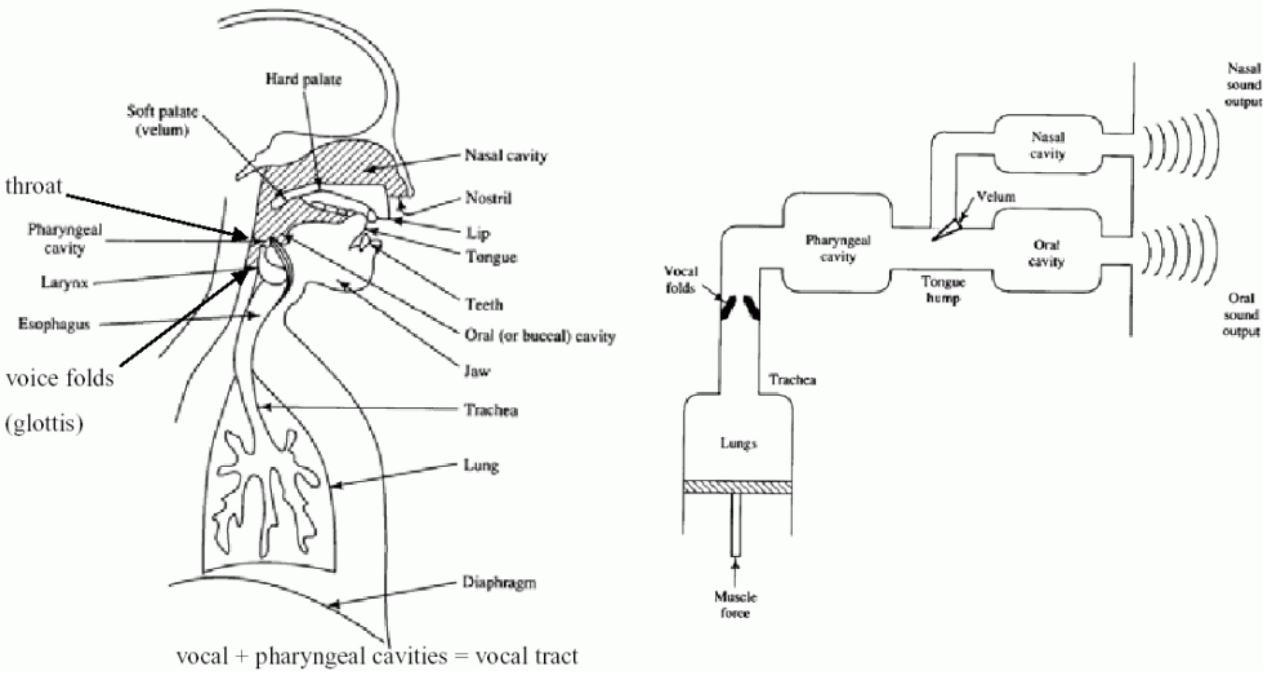

Fig-3.2 Speech Production through Human Throat

Speech sounds result are driven from a combination of the real source of sound energy (the larynx) modulated by a time-varying transfer function filter (vocal articulators) determined by the shape and size of the vocal tract. This results in a filtered spectrum with broadband energy peaks. This model is known as the source-filter model of speech production shown. In this model the source of acoustic energy is at the larynx, and the vocal tract serves as a time-varying filter whose shape determines the phonetic content of the sounds.

The Source Model

The source signal [3][4] of speech is the noise-like air from the lungs which is temporally and spectrally shaped by the manner and the frequency of the openings and closings of the glottal folds. There are two broad types of speech sounds as shown: *voiced* sounds like an "*e*" pronounced as "*iy*", and *unvoiced* sounds like "*s*".

Voiced sounds are produced by a repeating sequence of opening and closing of glottal folds with a frequency of between 40 (e.g. for a low frequency gravel male voice) to 600 (e.g. for female children's voice) cycles per second (Hz) depending on the speaker, the phoneme and

the linguistic and emotional/expressional context. First, as the air is pushed out from the lungs the vocal cords are brought together, temporarily blocking the airflow from the lungs and leading to increased sub-glottal pressure. Talking about the the sub- glottal temperature became greater than the resistive offereing by the vocal folds, the folds open and should be out a pulse of air. The folds then close rapidly due to a combination of factors, including their elasticity, laryngeal muscle tension, and the Bernoulli effect of the air stream. With this If the process is being maintained with a steady supply of pressurized air, the vocal cords will continue to open and close in a quasi-periodic fashion. As they open and close, the pulses of air flow through the glottal opening as shown.

The periodicity of the glottal pulses determines the fundamental frequency (*F*0) of the paramedical laryngeal receipting source and added to the perceived pitch of the sound. The time-variations of glottal pulse period convey the expressional content, the intonation, the stress and emphasis in speech signals. In normal speech the fundamental frequency (pitch) changes constantly, providing linguistic and speaker information, as in the different intonation patterns associated with questions and statements, or information about the emotional content, such as differences in speaker mood e.g. calmness, excitement, sadness etc. as shown in figure (3.3).

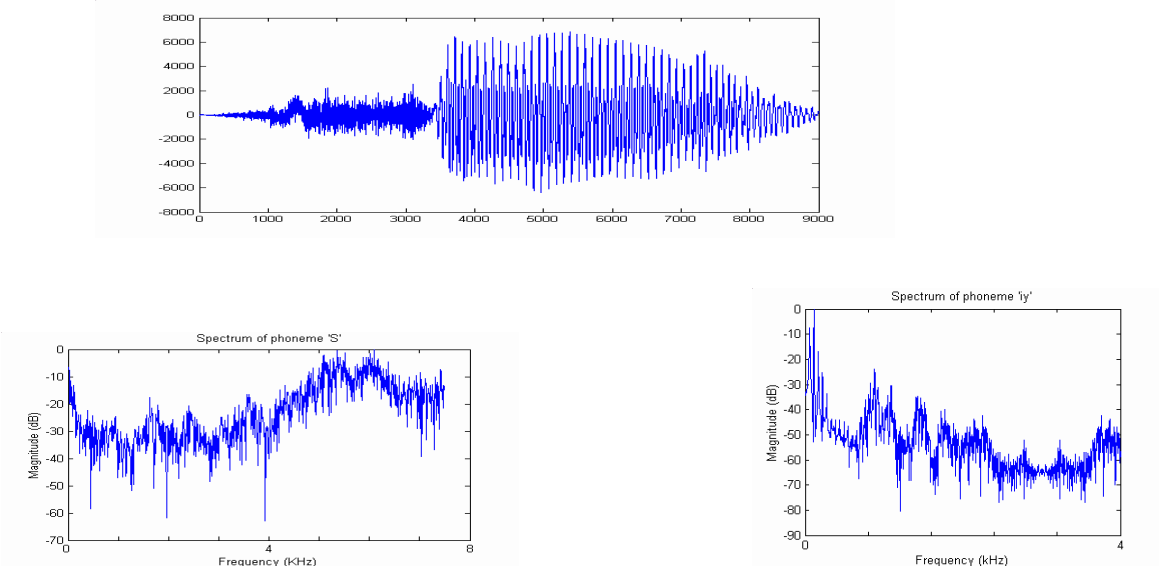

Figure-3.3 shows an example of a speech segment containing sound “s” & “iy”

Note that the spectrum of voiced sounds is shaped by the resonance of the vocal tract filter and contains the harmonics of the quasi-periodic glottal excitation, and has most of its power in the lower frequency bands, whereas the spectrum of unvoiced sounds is non-harmonic and usually has more energy in higher frequency bands. The shape of the spectrum of the input to vocal tract filter is determined by the details of the opening and closing movements of the vocal cords, and by the fundamental frequency of the glottal pulses.

For unvoiced sounds (such as consonants) air is passed through some obstacle in the mouth, or is let out with a sudden burst. The position where the obstacle is created depends on which speech sound (i.e. phoneme) is produced. During transitions, and for some mixed-excitation phonemes, the same air stream is used twice: first to make a low-frequency hum with the vocal cords, then to make a high-frequency, noisy hiss in the mouth.

3.1.3 Fundamental Frequency (Pitch) Estimation

Traditionally the fundamental frequency (whose sensation is known as pitch) is derived from the autocorrelation function as the inverse of the autocorrelation lag corresponding to the second largest peak of the autocorrelation function. Figure 13.10 shows a segment of voiced speech and its autocorrelation function. Note that the largest peak happens at the lag zero and corresponds to the signal energy. For a periodic voiced speech signal the second largest peak occurs at the lag T_0 corresponding to the period of speech.

The autocorrelation of a periodic signal is periodic with a period equal to that of the signal. Hence all the periodic peaks of the autocorrelation function can be usefully employed in the pitch estimation process as in Griffin's methods where the pitch period is found by searching for the value of period T that maximizes the following energy function.

3.2 Pitch Detection

3.2.1 Pitch detection in Time domain [6]

There are two methods for pitch detection as follows [6]

3.2.1.1 Auto Correlation Method

Autocorrelation is the cross-correlation of a signal with itself. basically, it is the similarity with observations as a function of the time separation between them. It is a mathematical tool for finding repeating patterns, such as the presence of a periodic signal obscured by noise, or identifying the missing fundamental frequency in a signal implied by its harmonic frequencies. It is often used in signal processing for analyzing functions or series of values, such as time domain signals as shown in figure (3.4).

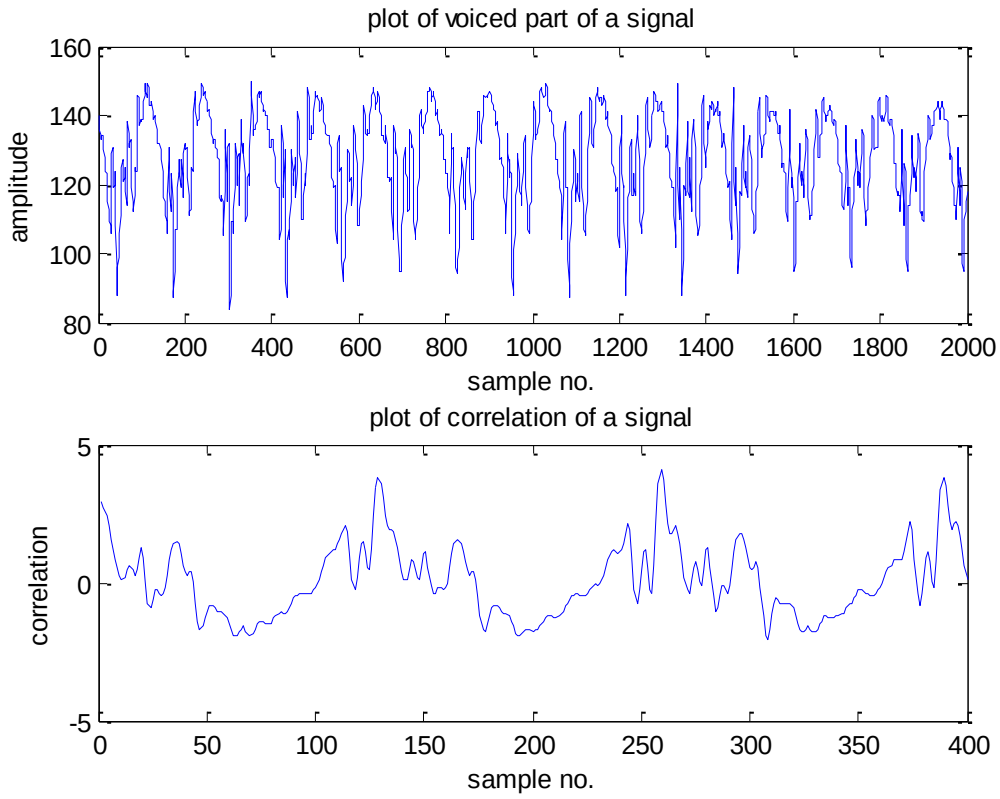

Fig-3.4 Plot of Voiced Part of Signal and plot of Correlation of a signal

$$Rxx = \lim_{N \to w} \frac{\sum_{i=0}^{2N} a(i) * a(i+k)}{2N+1}$$

Where $a(i)$ is the sample number and k is the interval and N is the total number of samples, R_{xx} is the resultant.

3.2.1.2 Average Magnitude Difference Method (AMDF)

We will start with the definition of average magnitude difference function. form the difference

signal by delaying the input speech by various amounts, subtracting the delayed waveform from the original and summing the magnitude of the differences between the samples values. Finally take the average of the difference function over the number of samples. The difference signal is always zero at delay=0. And is particularly small at delays corresponding to the pitch period of a voiced sound having a quasi-periodic structure. The main advantage of the AMDF method is that it requires only subtractions.

$$AMDF\ (k) = \frac{\sum_{i=1}^{N} abs[a(i) - a(i+k)]}{N}$$

Where *a(i)* is the current sample and *N* is the total number of samples and *k* is the interval.

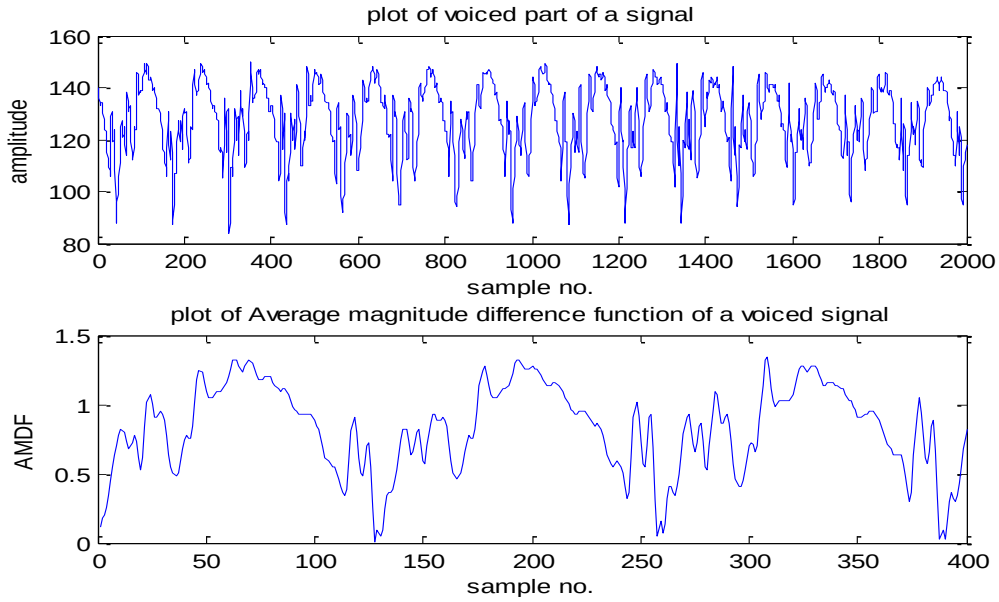

Fig-3.5 Plot of Voiced part of a Signal and plot of Average Magnitude Difference Function of a voiced Signal

3.2.2 Parallel processing approach for calculation of pitch frequency

Speech synthesis requires pitch detection and a (V/UV) decision making algorithm as the essential elements. This task requires a combination of signal processing and feature extraction. I will focus on an algorithm for pitch detection (V/UV) decision making in the time domain. All the present time domain algorithm fo pitch period measurement detect the peak, which is not only positioned at the correct pitch, but also at its integer multiples, thereby creating a possibility of

getting multiple and half pitch errors. This possibility can be eliminated using the parallel processing approach. This processing blocks work simultaneously to track pitch estimate.

3.2.3 Pitch Measurement in Spectral domain

i have studied time domain approaches for pitch period measurement .this section is devoted to the frequency domain approach for pitch period measurement. The frequency domain pitch detection algorithm operate on the speech spectrum . the periodic signal will have a harmonic structure. This frequency domain algorithm tracks the distance between the harmonics. The main drawback of the frequency domain method is its high computational complexity. We will describe for different methods for finding fundamental frequency using the spectrum as listed below-

1) FFT based method
2) Harmonic Peak detection method
3) Spectrum Similarity method
4) Spectral Autocorrelation method

3.2.4 Pitch period measurement using Cepstral domain

This section is devoted to the Cepstral domain approach for pitch period measurement. Let us first define a cepstrum. A cepstrum is obtained when taken the Fourier transform of the log spectrum. The name cepstrum is derived from the reversing the four letter of spectrum .it can have a power Cepstrum or a complex cepstrum.

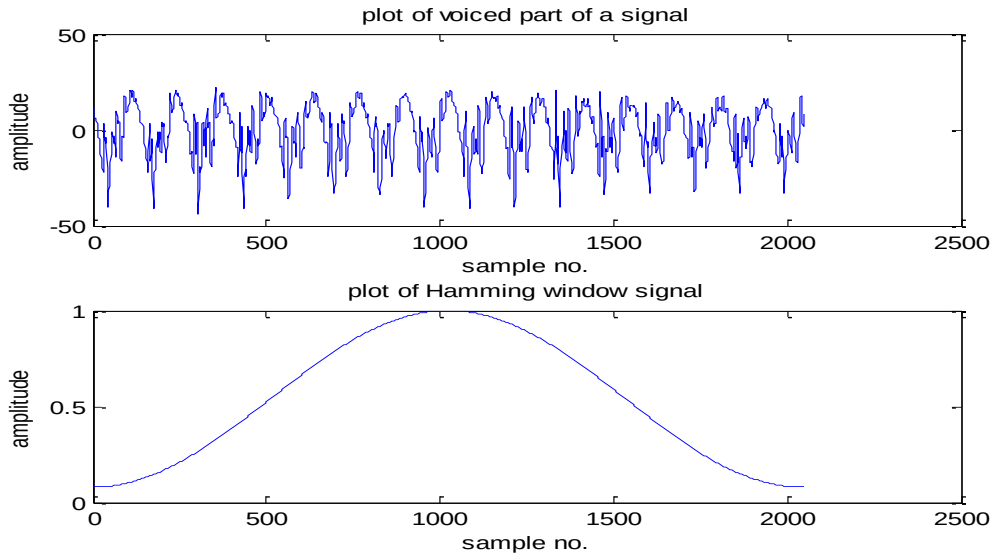

Figure 3.6 Plot of 2048 samples of voiced speech and Hamming window function

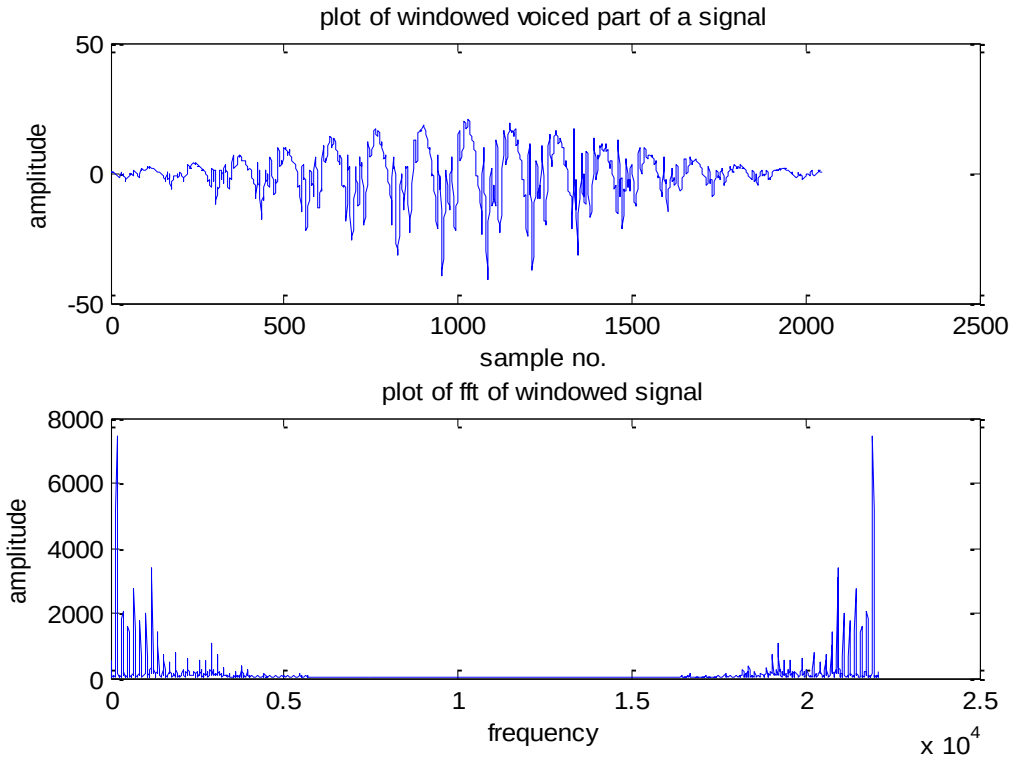

Figure 3.7 Plot of 2048 samples of Hamming windowed voiced speech and its FFT

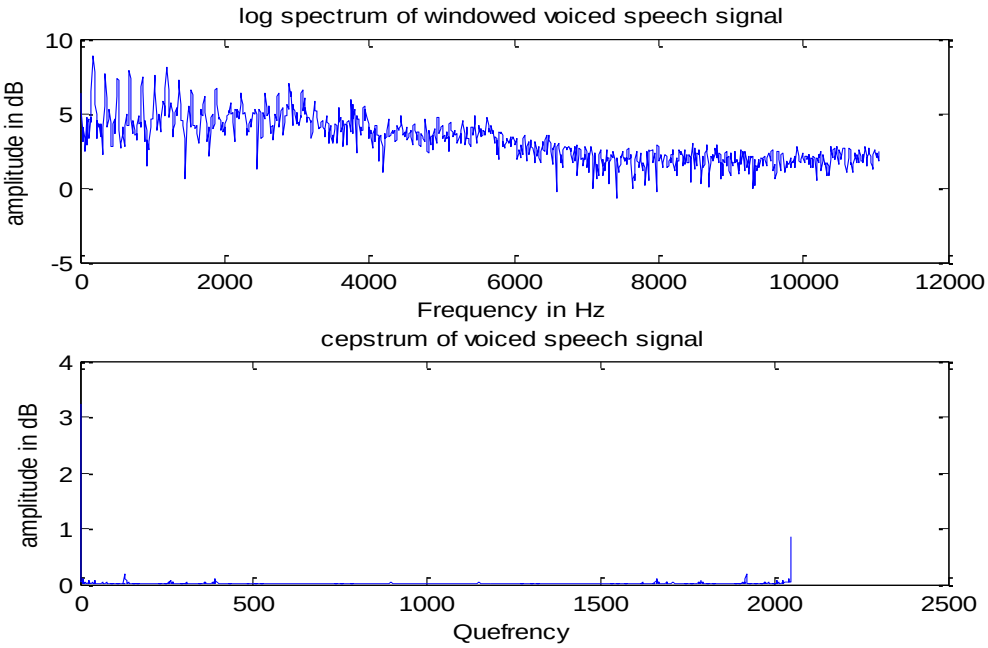

Figure 3.8 plot of log spectrum of 2048 samples of voiced speech and its Cepstrum

The algorithms take the FT of a signal followed by its absolute value and logarithm, thereby remaining in the spectrum domain that is the x axis denotes frequency. When take IDFT further actually come back to the time domain. But here there is a logarithm block in between which says that the output domain is neither a frequency domain nor a time domain. It is popularly known as the quefrency domain by reversing the words in frequency. Hence a cepstrum graph of a signal will be amplitude vs. quefrency graph.

When a signal is analysed in the cepstral domain, it is termed as cepstral analysis. A short time cepstral analysis was proposed by Schroder and noll for pitch determinationof human speech.

3.3 MFCC (Mel Frequency Cepstrum Coefficients)

3.3.1 Mel Scale

Computation of the Short Term Spectrum

As recalled, it is necessary to compute the speech parameters in short time intervals to reflect the dynamic change of the speech signal. Typically, the spectral parameters of speech are estimated in time intervals of 10ms. First, i have to sample and digitize the

speech signal. Depending on the implementation, a sampling frequency f_S between 8kHz and 16kHz and usually a 16bit quantization of the signal amplitude is used. After digitizing the analog speech signal, got a series of speech samples $s(k \cdot \Delta t)$ where $\Delta t = 1/f_S$ or, for easier notation, simply s(k). Now a reemphasis filter is used to eliminate the -6dB per octave decay of the spectral energy:

The **Mel scale [13][14]**, named by Stevens, Volkmann and Newman in 1937 is a perceptual scale of pitches judged by listeners to be equal in distance from one another. The reference point to this scale and normal frequency measurement is defined by assigning a perceptual pitch of 1000 mels to a 1000 Hz tone, 40 dB above the listener's threshold. Above about 500 Hz, larger and bigger intervals are measured by audience to produce equal pitch incremental. As a result, 4 octavers on the mel scale above 500 Hz when judged to consist about two octavers on the hertz scale. The name **mel** comes from the word **melody** to indicate that the scale is based on pitch comparisons.

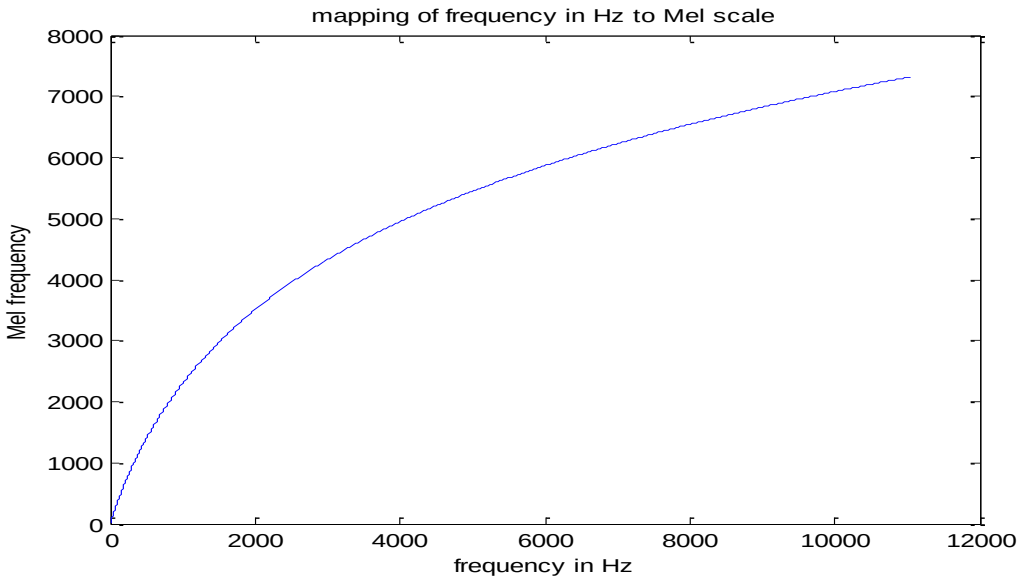

Fig-3.9 Mel Frequency Scale corresponding to Normal Frequency Scale.

A popular formula to convert f hertz into m mel is

$$MelFrequency = 2595 * \log(1 + \frac{F}{700})$$

MEL Frequency Cepstrum

In sound processing, the **Mel-frequency Cepstrum** (**MFCepstrum**) is a indication of the short-term power spectrum of a digital sound, based on a basic linear cosine transformation of a linearlog power spectrum on a nonlinear Mel scale of frequency.

3.3.2 Generation of Mel Cepstrum Coefficients

Mel-frequency cepstral coefficients (**MFCCs**) are that collectively build up an MF Coefficients. They are derived with a linear type of cepstral representation will be the of the audio layer (a nonlinear "spectrum-of-any-spectrum"). The difference between the linear Cepstrum and the Mel-frequency Cepstrum is that in the basic MFC, the frequency bands are equally spaced on the Mel scale, which equivalently the human auditory system's responsiveness more similarly than the linearly-spaced frequency basic details bands used in the normal Cepstrum. This frequency moving warping can allow for better representation of digital sound, for example, in audio compression.

MFCCs are commonly derived as follows:

1. initialize the Fourier transform [14] of (a windowed excerpt of) a signal.
2. Start the powers of the spectrum obtained above onto the mel scale, using triangular overlapping windows.
3. Start the logs of the powers at each of the mel frequencies.
4. Start the discrete cosine transform of the list of Mel log powers, as if it were a signal.
5. Basic details of MFCCs are the amplitudes of the resulting spectrum.

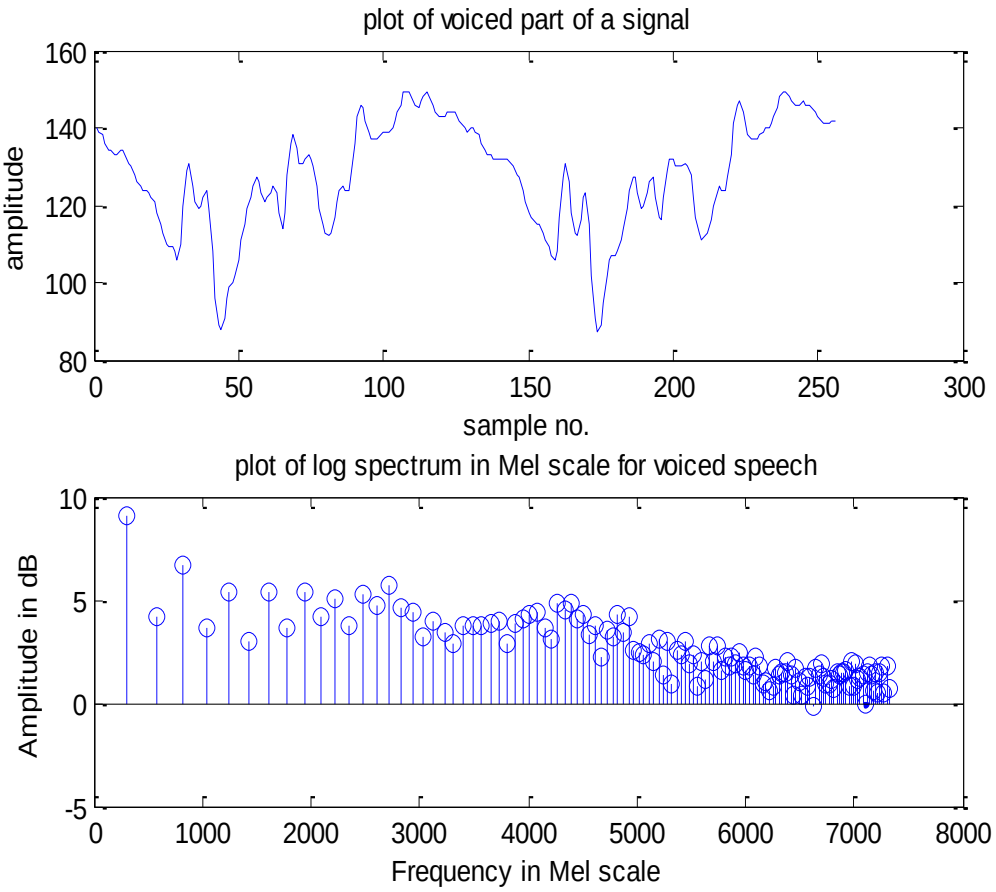

Figure 3.10 Plot of speech and its log power spectrum for each fft point on mel scale.

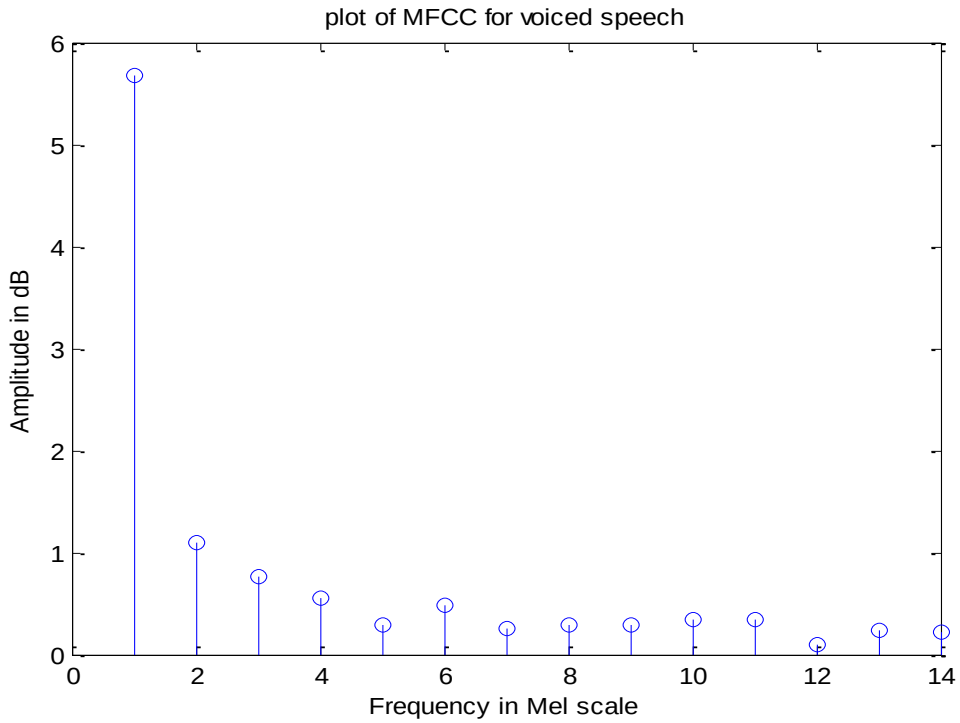

Figure 3.11 Plot of 14 MFCC points.

There may be variations of this process, for example, differences created in the shape or spacing of window of the windows used to map the scale. The European basic tele-details Telecommunications Standards Institute in the early 2000s defined a standardized MFCC algorithm to be used in mobile phones.

Chapter 4

PROPOSED SYSTEM

4.1 Two layer Approach

The main area of interest of this paper is here because it has two layered approach and applied this on an image in secure transferring over network. It has to be finding Mel frequency Cepstrum coefficients with the above given formulas. So here one speech segment has been taken.

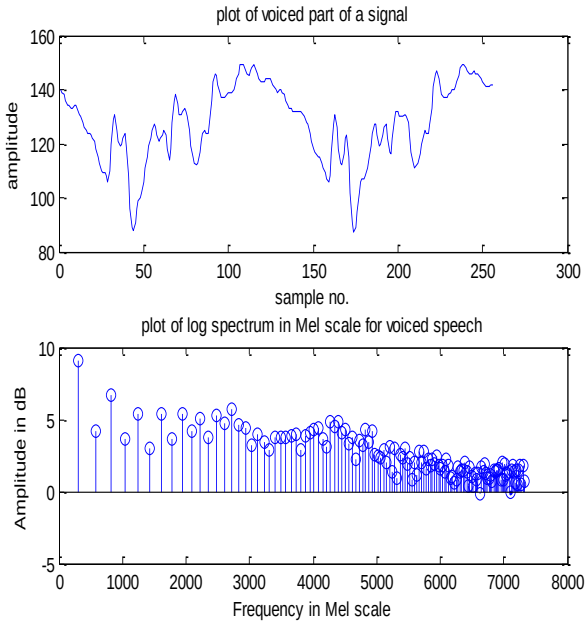

Fig-4.1 Plot of voiced part of a signal and plot of log spectrum in mel scale for voiced speech

One speech segment has been taken and finds its voiced part first and then finds the log spectrum in Mel scale frequency and got above given plot of that result. Now it has to find the MFCC for voiced speech then below given graph is showing that 14 coefficients that are getting and they are plotted as follows.

4.1.1 Calculate MFCC and Pitch

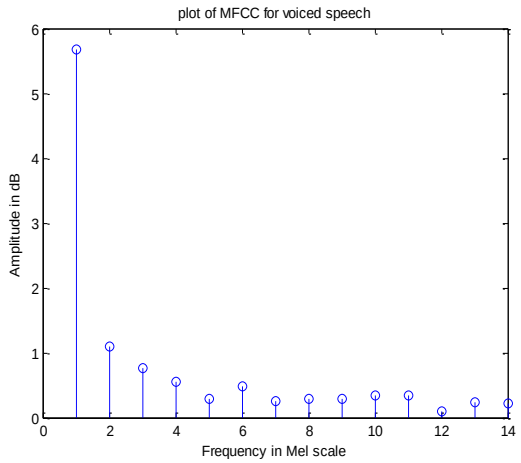

Fig-4.2 Plot of MFCC for voiced Speech

An array of 14 coefficients are there which are as follows 5.6999, 1.0993, 0.7545, 0.5487, 0.2899, 0.4800, 0.2525, 0.2825, 0.2831, 0.3480, 0.3459, 0.1003, 0.2398 and 0.2271. If there is to plot a graph for this then the graph will show actual flow of the data in voiced part. It can also find these coefficients from MATLAB command 'melcepst' from voice box, but you have to first install that tool box into your MATLAB software. Now it has to perform operation and apply these coefficients and pitch value to an image with this approach-

$$R = \sum_{i=1}^{14} \left(\frac{Xi}{14}\right) * \mathrm{P}$$

Where X_i is the coefficients and P is the pitch value and R is the resultant. To Apply this result in a 2D image given below. In this thesis, a efficient method is shown to derive Mel-frequency cepstral coefficients very much directly from the power spectrum of a voice/speech wave signal. It is looking that removing the filter-bank in signal direct gazing analysis never affects the word fault-rate. The dedicated approach shows the speaker's front end by combining subsequent signal analysis steps into a single signal. It is avoiding possible criteria and discretization difficulties

and results in a compact merging and implementation. It is represented that frequency attiring schemes like vocal tract normalization can be combined early in their concept without additional computational efforts. Basic identification test results obtained with the large vocabulary voice recognition system is presented for basic two different corpora: The russian VerbMobil II dev99 corpus, and the English. Most of the day automatic voice recognition systems are based on some type of Mel-frequency basic view of cepstral coefficients (MFCCs), which is proved to be more effective and efficient under various conditions. This thesis describes an alternative concept to derive basic view of multidimensional MFCCs directly from the basic power spectrum of the speech signal analysis. A number of starting point of view steps of the very much old signal analysis are combined into the cepstrum transformation, which avoids possible discretization and interpolation faults and errors. The very much old and new concept outputted equally good recognition criteria performance without a filter-bank, thus reduces the number of parameters that which are needed to be optimized. The remainder of this research is organized as follows: In the next section it will briefly recapitulate the typical signal analysis procedure. Then discussed in detail implementation issues of the old and new MFCC computation and past and present our integrated approach and analysis.it will be easily demonstrated that basic frequency modeling warping schemes like vtn can be easily integrated and combined as well as . Finally, it will be present recognition test results for the and the south American Business ans consultant News Corpus, and basic application of drawing the conclusions of our work system. The speech waveform and caused to be, sampled at 9 or 15 kHz, is first differentiated and cut into a number of overlapping parts or called as segments, each 24 ms long and shifted by 11 ms. A Hamming window will be multiplied and the fast Fourier transform (FFT) is calculated for each frame. The power spectrum is combined and warped according to the Mel-scale in order to adapt the frequency resolution to the real and remaining properties of the human auditory system. Then the spectrum is segmented into a number of critical bands by means of a filterbank. The filterbank typically consists of overlapping triangular filters. A discrete linear cosine transformation of the basic function limit (DCT) applied to the logarithm of the filter-bank algorithms for better outputs results in the raw MFCC vector. The highest cepstral coefficients are omitted to smooth the cepstra and minimize the influence of the pitch which is irrelevant for the speech recognition process. The mean of each cepstral component is subtracted, and the variance of each component

may also be normalized. Finally, the MFCC vector is augmented with time derivatives. Additional transformations like linear discriminant analysis (LDA) may further increase the temporal context and the discriminance of the acoustic vector. As a result signal analysis provides every 10 ms an acoustic vector, which is typically of dimension 25 to 50.

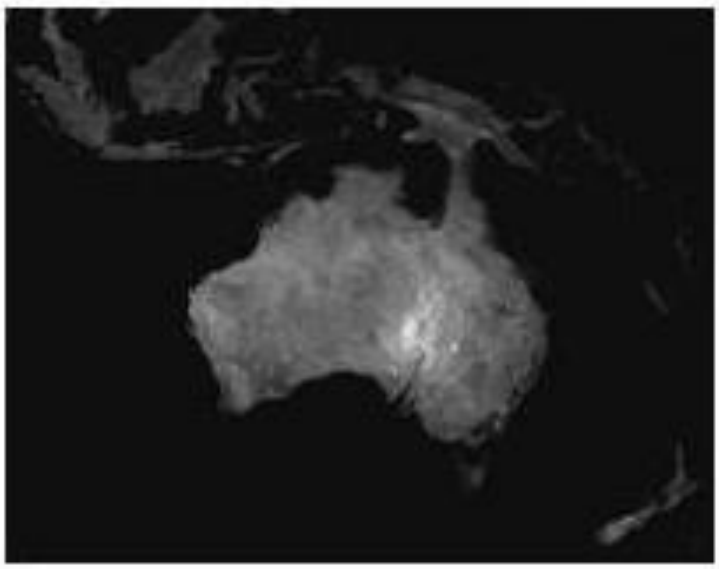

Fig-4.3 Original Satellite Image of Australia Image

4.1.2 Apply MFCC & Pitch on Image

For applying on each pixel of the image, function is called

MFCC-on-IMAGE (A[N][M], R)

```
Step-1 for (i=0 to N-1)
    {
      For (j=0 to M-1)
        {
          A[i] [j] =A [i] [j]*R;
                              }
          }
```

Step-2 Traverse on each pixel value of the image to locate the pixel value.

Step-3 End;

After apply this approach, got some result which are shown below.

Where i and j is the pixel values at x axis and y axis respectively. It has been got from above mentioned formula. After applying MFCC value and pitch value our image get distracted and will be noisy that is also good for secure transferring over network. Here result of image is purely black and no one can identify any thing in the resultant image. Further this will find it's histogram for see the changes after performing operation.

Fig-4.4 MFCC coefficients and pitch value applied on Image

4.1.3 Apply ECC Encryption on Resultant Image

Now it has to apply ECC (Elliptic Curve Cryptography) on this output image and then transfer over network, so now task is how to encrypt the image with ECC Encryption so it has to be understand some points about ECC Encryption they are as follows-

- ECC is a public key algorithm which works on private key and public key.
- ECC designed and mainly used for handheld devices and small devices which are low in memory and resources.
- ECC successfully implemented first by Koblitz and miller [10].

- ECC encryption uses elliptic graph, onto this graph which points are generated that are taken for encryption.
- Main use of ECC is for those devices which can work only in constrained environment.

There is two operations involved in ECC which are (1) Point Multiplication [11] which internally consists two operation i.e., point addition and point doubling, in point doubling it doubles the point which is of same kind with point doubling formula i.e., say one point is $T(X_T, Y_T)$

$L(X_L, Y_l)=2T(X_T, Y_T)$

$X_L=S^2-2X_T \bmod p$

$Y_L=-Y_T+S(X_T-X_L) \bmod p$

$S=(3X_T^2+a)/(2Y_T) \bmod p$

Where S is the tagent at point T and a is one of the parameter chosen with the elliptic curve and p is a prime number.

Now in point addition it is used for addition of two points with point addition formula i.e., say two points $P(X_P, Y_P)$ and $Q(X_Q, Y_Q)$ then $I(X_I, Y_I)$

$X_I= S^2-X_P-X_Q \bmod p$

$Y_I= -Y_P+S(X_P-X_I) \bmod p$

$S=(Y_P-Y_Q)/(X_P-X_Q) \bmod p$

Where S is the tagent passing through P and Q and p is a prime number.

ECC point generation

According to elliptic curve $y^2=(x^3+ax+b) \bmod p$ where $4a^3+27b^2\neq0$ some points should be generated that lies on elliptic curve. Let p=39, a=-1, b=1 on which 'a' and 'b' value satisfying above equation. Encryption is to be done first so generate all points that satisfies the elliptical curve follow this function **GeneratePoints (a, b, p)**

Step 1 take x=0 or any other positive integer

Step 2 loop until x<p

I. $Y^2=(x^3+ax+b) \bmod p$

II. If y^2 is perfect square

Print(x, square root (y))

Else

x=x+1;

Step 3 End

where p is a prime number, x and y are co-ordinates.

ECC Encryption

Step 1-For all P_I (pixel value)

Find $S=P_I * AF_M$ //*P_I is constant, AF_M is random Affine- point in elliptic curve. *//

Step 2- Find $PK_B=PRK_B*BP$ //*B_P is the base point Of Elliptic curve, PRK_B is the private key. *//

Step 3- End;

Encrypted data= (N*BP, $S+N*PK_P$)

4.1.4 Reverse Operation

ECC Decryption

Follow this method for decryption,

Let N*BP be the first point and ($S+N*PK_B$) be the second point PRK_B *N*BP=PRK_B *first point

Calculate $S=S+N*PK_B-PRK_B*N*BP$

Calculate the scalar value of 'P_I' from S_M using discrete logarithmic problem [7]. Where PK_A, PRK_A and PK_B, PRK_B is the public key and private key of user A and B respectively.

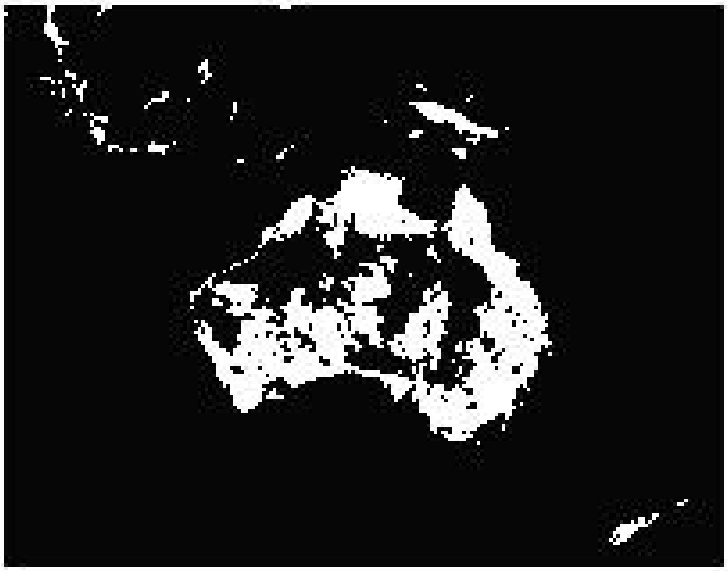

Fig-4.5 after ECC decryption of Image

In decryption of the ECC it will use the discrete logarithmic Problem, after applying on each pixel, got all the decrypted 2D-matrix i.e., image. Below histogram is shown of above image and can analyze this histogram with original image's histogram. It is approximately same.

Above shown image is the decrypted image after Discrete Logarithmic problem [7]. Now this image got at the receiver side but it has to follow one operation also i.e., remove the MFCC coefficients from encrypted image then got our real image.

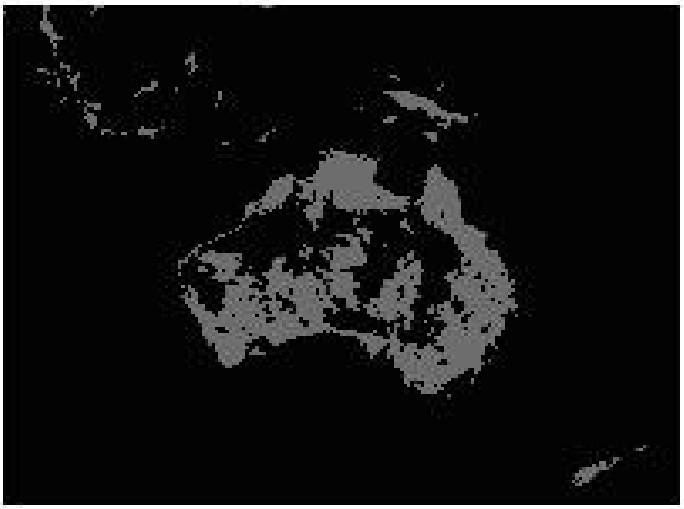

Fig-4.6 Remove MFCC and Pitch from Original Image

Here just apply reverse operation for removing the MFCC and pitch value. Now analyze our result image maximum feature of the image can be identified and this method is better working for satellite image further more operation can be performed on the resultant image if image is to be enhanced.

4.2 Advantages of Proposed System

As it is known very well use of images in now days is very much, in area of cryptography, in area of forensic science, in daily life and images is the best option to hide the data and transfer over network. Main concern in today's life is to secure the images and authentication of genuine images is very much. Image should be protect from hackers and authenticate whether the sender is genuine or not and also to maintain the integrity of the data. In information security there are many algorithms which are used for authentication such as digital signature; digital certificate etc. in this paper a new idea is proposed for protecting the image from MFCC coefficients.

According to the paper one sample voice segment has been used and finds the MFCC coefficients and apply on image and then encrypting the image through MFCC and all knows very well that each human's voice is unique and MFCC also used for speaker verification so at the receiver side when same MFCC coefficients from same voice has been found then remove MFCC feature from the image and then verify our image is that it is coming from genuine user or not. If anyone alters the message in between the network then real image will not recover. Some malfunctioned image has been get and then that image will not be accepted so with this it also maintain the message integrity. So with MFCC coefficients image authentication and message integration can be done.

Chapter 5

RESULTS AND ANALYSIS

5.1 Satellite images

5.1.1 Description about satellite Images [17][18]

The first images from spaces were taken on sub-orbital flights. The US-launches V-2 on October 24, 1946 took each image every 2.5 seconds. With an apogee of 65 miles (105 km), these pictures were five times higher compare to the last record, the 13.7 miles (22 km) by the Explorer II balloon mission in 1935. The very first satellite image pictures of Earth were made on August 1959 by the US. The first satellite photographs of the Moon might has been made on October 1959 by the Russian satellite Luna 3, on a aim to picture the far side of the Moon. The Blue Marble pictures was taken from space in 1972, and has become very famous in the e-media and between the people. Also in 1972 the United States commenced the Land--sat program, the biggest program for achievement of images of earth from universe. Land--sat Data Continuity aim, the very much recent Land--sat satellite, was started on February 2013. In 1977, the very first real feel time satellite imaging was achieved by the USA satellite management system. All satellite images produced by NASA are published by Earth Observatory and are freely available to the public. Several other countries have satellite imaging programs, and a collaborative European effort launched the ERS and Envisat satellites carrying various sensors. There are many other also other companies that giving commercial satellite imaging. In the early century satellite imagery become very much available when are in budget, easy to use software with accessing to satellite imaging records was offering by several organizations

5.1.2 Uses of Satellite Images

Satellite images [17][18] have many applications in meteorology, agriculture, geology, forestry, landscape, biodiversity conservation, regional planning, education, intelligence and warfare. Images can be in visible colors and in other spectra. There are many elevation maps, generally made by radar. Interpretation, implementation and analysis of satellite imaging was conducted using special remote sensing/analysis applications. Very few of the first image restoration of

satellite pictures was launched by the US Government and its relators.. For example ESL Incorporated developed some of the earliest two dimensional Fourier transforms applied to digital image processing to address NASA photos as well as national security applications. Satellite imagery is also used in seismology and oceanography in reducing effects to land de-formation, water depth and sea bed-loom, by very much color caused by earthquakes, volcanoes, and natural disaster.

5.1.3 Resolution & Data

In this there is 4 types of resolution images when discussing satellite imaging in remote sensing/analyzing: spatial, spectral, temporal, and radiometric. The record of Campbell (2006) defined as follows: - spatial resolution was defined for the pixel size of an image representing the size and location of the surface area is being counted on the land, determined by the sensor's instantaneous field of view can be said as (IFOV); - spectral resolution is defined by the wavelength interval size (discreet segmentation of the Electro-magnetic Spectrum/resolution) and number of intervals/breaks that the sensor is mapping; temporal resolution/brightness is defined by the amount of time that passes between imagery collection periods for a given surface location; and radiometric resolution/imaging is explained is the capability of an imaging system to record many levels of resolution/brightness. – Radiometric data resolution references to the good effectiveness bit-depth of the sensors/analyzers (grayscale levels images) and is very much typically expressed as 8-bit (0-255), 11-bit (0-2047), 12-bit (0-4095) or 16-bit (0-65,535). - Geometric resolution references to the satellite sensors capability to precisely imaging a portion of the Earth surface in a very single pixel and is difficultly expressed in terms of Ground Sample Distance meter, or GSD. GSD is a term containing the overall optical and systemic noise sources and is useful for comparing how well one sensor can "see" an object on the ground within a single pixel. For example, the GSD of Landsat is ~30m, which means the smallest unit that maps to a single pixel within an image is ~30m x 30m. The latest commercial satellite (GeoEye 1) has a GSD of 0.41 m (effectively 0.5 m due to United States Government restrictions on civilian imaging).

The resolution of satellite images varies depending on the instrument used and the altitude of the satellite's orbit. For example, the Landsat archive offers repeated imagery at 30 meter resolution for the planet, but most of it has not been processed from the raw data. Landsat 7 has an average return period of 16 days. For many small areas, images with spectrum/-resolution as high as 40 cm may be available. Satellite imagery is sometimes replaced with aero-logical imaging, which has higher resolution, but is more expensive per square meter. Satellite imagery can be merged for with vector or raster data in a GIS provided that the imagery had been spatially refined so that it will properly align with other data sets.

The use of satellite imagery in everyday life is by no means a novelty. Since the first satellites dedicated to imaging land areas were placed in orbit in 1972 (Landsats), weather reports have become about the most recognizable by-product of humanity's optical dominance of the earth's atmosphere. The excitement and curiosity of viewing our planet from afar has recently led to propositions of sending satellites far into stellar orbit simply to have a live image of our planet. Anyone with a personal computer and modem can, in minutes, have a near-instant satellite image of almost any part of the globe. The rapid advances and accessibility of computer technology has placed satellite technology in millions of homes, cars, schools, and offices. The potential practical use of this technology by amateur and other non-technically expert institutions and individuals is only now beginning to surface.

This essay elaborates a series of issues, legal, economic, social, and practical, which arise (or would arise) in the uses (or potential uses) of satellite imagery in the field of human rights. Given the limited experience to date with the application and use of satellite imagery for human rights promotion and protection, the work is exploratory and attempts to develop inroads to using satellite imagery in monitoring human rights conditions and enforcing international human rights legislation. The essay identifies theoretical and legal frameworks in which such use would occur, potentially interested parties, specific territorial issues, technological as well as financial implications which define the types of uses, general accessibility, etc.. As this is a new area of exploration, much of the material presented is hypothetical, and should be used as a guideline or framework for further research on this topic. It should not be viewed as definitive or exhaustive.

Linking Human Rights and Environment2 Probably the most obvious use of satellite imagery, or at least the one that comes most immediately to mind, is by its very nature, environmental. What we see from high above the earth is indeed "the environment", our earth, our waters, our wildlife, our air, ourselves. Because, as a global society, we are ever more concerned with the transformations our planet is undergoing due to our own uncontrolled use of natural resources, we have become interested in monitoring our environment, identifying trends in resource depletion, and identifying problem areas. Space provides us a privileged Jorge Daniel Taillant is a specialist in subnational development and urban specialist. He is Development Director of the Center for Human Rights and the Environment, in Córdoba Argentina. Romina Picolotti is a Specialist on Human Rights and is Executive Director of the Center for Environment and Human Rights. See CEDHA, Center for Human Rights and Environment. viewpoint, as it allows us to look at ourselves from a global or "bio spherical" perspective, i.e. as a whole "natural" unit, the earth. Yet despite the generally accepted view that the environment is the critical framework for our sustainable development, we fail to include ourselves as a fundamental component of our environment. The environment is our habitat, and therefore, that which affects the environment, affects us directly. The environment, however, is largely and most commonly addressed as a natural habitat, comprising land, waters, and wildlife. We, humans, often see ourselves as somehow removed inhabitants of the environment, despite our inherently organic insertion into its ecology. The depletion of our natural resources affects our access to those resources. Contamination to our environment affects our habitat, and consequently affects our living conditions, and ultimately our rights as humans to a healthy environment and basic living standards. We are in the end, although we may not treat ourselves as such, an inseparable element that within our environment and affected by it. Abuses to our environment, hence, are abuses to us and to our human rights. Earth Use and Satellite Imagery Satellite imagery, beyond registering images of the natural earth, especially when these can be observed over a time series, registers a unique perspective on the use of natural resources, land, forest, waters, air, etc.. This use, which we will call "earth use" includes habitation patterns, (urbanization vs. realization) as well natural phenomenon, and the exploitation of natural resources which can be perpetrated by governments, companies, institutions, organizations, individuals, or wildlife. Earth use, sustainable or unsustainable, we know and agree, is of

fundamental concern to environmental Sustainability, and subsequently, of great concern to our basic human rights. The way in which the earth is, or can be, potentially "used" is multifaceted, and involves many actors and interacting dynamics. For the purpose of analysis, we can examine earth use from a variety of optics, legal, economic, political, social, or moral (to name a few), each of which will shed light on a series of issues, affected or participating actors, arenas, 5 with corresponding and particular social and environmental consequences. Legally speaking, earth use may be legal or illegal according to local or international legislation. Economically, earth use may add or detract from economic productivity, improving or deteriorating human condition. Politically, earth use may be more or less politically viable, or a given political decision can influence how the earth is used. Socially, we may have ideas about how a given earth use can best benefit or harm a given sector of the population. Morally, as a society we may have opinions about how the earth should be exploited, at what cost, and just what earth use should or should not be allowed, beyond a mere legal reference. These optics are merely a reference to be used in approaching earth use, which can help us define parameters for assessing the consequences, and help the determine the stakeholders and their positions with respect to the earth use in question. Satellite images, hence, assist us in mapping earth use, either at a given time or over a specific time interval. In terms of our optics, satellite images can help us categorize and value the various consequences of earth use at any given time or over a time period. Satellite images of earth use can act as a tool to monitor this use, linking the normative to the practical and cultural, helping us analyze, verify, and assure that, in practice, our earth use, is in line with our legal, social, economic, moral and political frameworks we have developed to make use of our natural resources and protect our human rights. And in the event our normative frameworks are hindering the promotion of a sustainable environment, satellite imagery may assist us to reconsider or reevaluate norms and regulations. Uses of Satellite Imagery for Human Rights Defense and Promotion To begin to address the uses of satellite imagery in promoting and protecting human rights, one must first technically understand just what these images provide in terms of pictorial definition, i.e. precisely what types of images are we talking about? While some geographic information systems (GIS) involving aerial photography taken by especially equipped airplanes, offer pinpoint accuracy, allowing a person to read a newspaper from a vantage point of up to many thousands of meters above the earth, most satellite images do not

allow for such precision definition. Pixel definition (point resolution) can be from under a meter in width to well over thirty meters. That is, in the case of one-meter resolution, one point in the given image represents a meter of image, so that any part of the image of less than a meter in size would not be recognizable in detail. Finer definition provided for by some GIS systems, might distinguish which finger on a hand has a gold ring on it, while others may only distinguish where one grove of trees ends and where another begins. To place our case for human rights uses of satellite imagery in perspective, a single "human", will likely not be identifiable via satellite imagery. This does not mean that lower resolution satellite imagery does not provide powerful data, but rather that the images that the vantage of the images it does provide lies in its ability to capture more macro data such as forest growth, general population displacements, movement of oil spills, etc.. Satellite images and other aerial photography is already widely used in Global Information Systems, such as in cadaster registrars, or in urban planning exercises. These data are used to determine population shifts, natural resource use, water displacements, and other changing earth patterns. For the most part, the use of satellite imagery in terms of earth use has been limited to monitoring environmental transformations, and in the case of urban planning, to land use in a strictly "urban" sense. Yet few cases exist where satellite imagery has been used specifically to explore the linkages of the changing environment to basic human rights. In order to bridge this gap, a greater social consciousness is necessary of the inherent links between our human rights and our habitat. Satellite imagery can serve as a measuring stick to monitor basic economic and social human rights. Taken to the field of the defense and promotion of human rights, it might be difficult to identify bodily harm inflicted on an individual, but it may be quite possible to identify mass graves (GIS systems, although not satellite images but rather airplane imagery, has been successfully used to identify mass graves), monitor intrusion into indigenous territories, or track the persecution of a tribal community or other human mass across a determined land area. Defending human rights from space implies difficult challenges in interpreting dynamic and ongoing change and action through the use of static single images. A single image, while potentially powerful (say a photograph of an oil spill or of mass graves), does not necessarily show causality, which is crucial in the legal sphere. A satellite image may merely bring a visible human rights issue to the attention of interested parties, and subsequently lead to investigation and eventual prosecution. If properly exploited, this propagandistic use of

satellite imagery may indeed be a useful contribution to the defense of human rights. Yet the sequential images that may be had from a time series of images from a given geographical area may nevertheless help shed light on the causality of events. The deforestation of a given area over time due to logging clearly shows causality. That is, the causality of logging and the deforestation viewed over time in satellite images is clear in the mind of anyone and need not suffer severe legal questioning. Taking the example a step further, if the causality implied by the viewed deforestation can be linked to government or commercial policy, and not only to the physical action of cutting trees, a solid case might be made identifying the responsible policy and actors of the witnessed action, and such causality can subsequently provide substantive material to present in court. The time factor of satellite imagery, that is the sequential images that may be taken over a given period of time (logging), versus the instantaneous image of a particular incidence (oil spill), reveals very different methodological uses and application of satellite imagery for protecting and promoting human rights. Cases of abuses requiring urgent action related to a specific incident, such as oil spills, fires, waste dumping, etc. can be buttressed by instant imaging, while sequential imaging can be used for prevention purposes by monitoring change in earth use, bringing evidence to build cases against purported violators of human rights and environmental abuses, and to enforce legislation or even review or reconsider the impacts of legislation. Below are some examples of instances or issues in which satellite imagery may contribute to the defense and promotion of human rights.

Now here are the results of all images which are got in the interval operations the first one is the original image (5.1) and after that we applied MFCC coefficients and pitch value and got result (5.2) figure. after that we applied encryption on the image and then we applied decryption then we got (5.3) figure. Finally we have to remove the MFCC coefficients and pitch information from our original image now we got (5.4) figure after apply last operation.

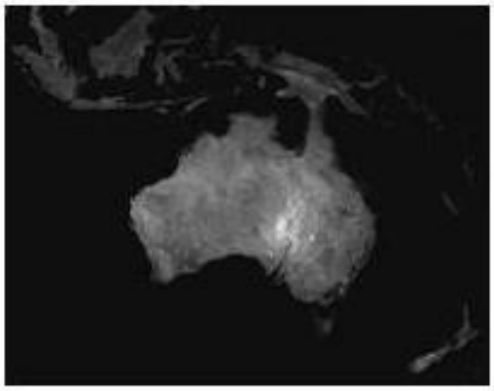

Fig-5.1 Original Image

Fig-5.2 MFCC coefficients and pitch value applied on Image

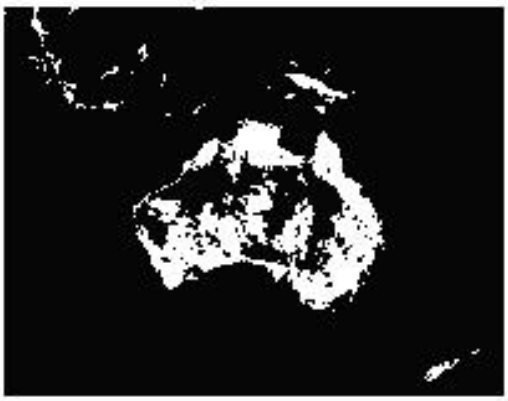

Fig-5.3 After ECC decryption of Image

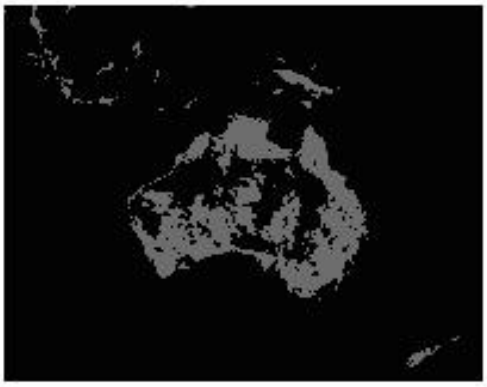

Fig-5.4 Remove MFCC and Pitch from Original Image

5.2 Histogram Analysis

In statistics, a **histogram** is a graphical representation of the random distribution of pixels. It is an estimate of the probability distribution of a continuous variable and was first introduced by Karl Pearson. A histogram is a representation of tabulated frequencies, shown as adjacent rectangles, erected over discrete pixels intervals, with an area that is very much equal to the representing frequency of the samples in the interval. The super height of a diagram rectangle is also very much same to the frequency distributor density of the pixels intervals, i.e., the frequency/repetition is divided by the width of the interval. The less total area of the histogram is equivalent to the number of pixels/data. A histogram can also be said displaying relative frequencies. It then shows the proportion of cases that fall into each of several categories, with the total area equaling one. The categories are usually specified as consecutive, non-overlapping intervals of a variable. The categories (intervals) must be adjacent, and often are chosen to be of the same size. The rectangles of a histogram are drawn so that they touch each other to indicate that the original variable is continuous. Histograms are used to plot the density of data, and often for density estimation: estimating the probability density function of the underlying variable. The total area of a histogram used for probability density is always normalized to 1. If the length of the intervals on the *x*-axis is all 1, then a histogram is identical to a relative frequency plot. An alternative to the histogram is kernel density estimation, which uses a kernel to smooth samples. This will construct a smooth probability density function, which will in general more accurately reflect the underlying variable.

The histogram is one of the seven basic tools of quality control. Histogram of the original image is describing that probability of the variable which is containing value 1 that is higher and white pixel quantity is very low. Our aim is that we have to give approximate equal histogram of original image and final image after applying operation. By the results we are looking that approximate equal histogram is displaying by the image. In the area of digital image processing, the histogram of a image simply references to a histogram of the pixel resolution/intensity values. This histogram is a graph relation representing the number of data values in an image at each different resolution value found in that image. As in-an 8 bit grayscale image there are 256 different various intensities/pixels values, and so the histogram will graphically display 256 numbers matching/showing the random distribution of pixels/intensities amongst those grayscale values. Histograms can also be taken of RGB (color) images --- individual histogram of red, green and blue scales can be taken, or a 3-D histogram can be produced, with the three axes representing the red, blue and green channels, and brightness at each point representing the pixel count. The very much clear output from the operation depending upon the implementation --- it may simply be a picture of the required histogram in a suitable image format, or it may be a data file of some kind representation of the histogram statistics as shown in figure (5.5,5.6,5.7,5.8).

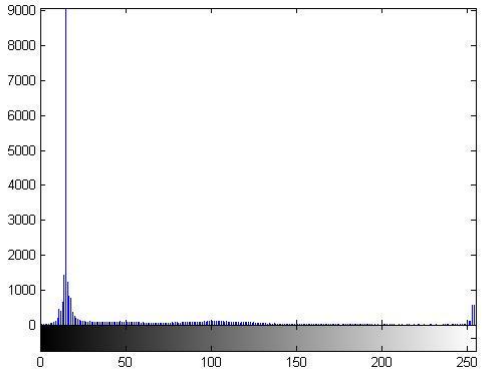

Fig-5.5 Histogram of Original Image

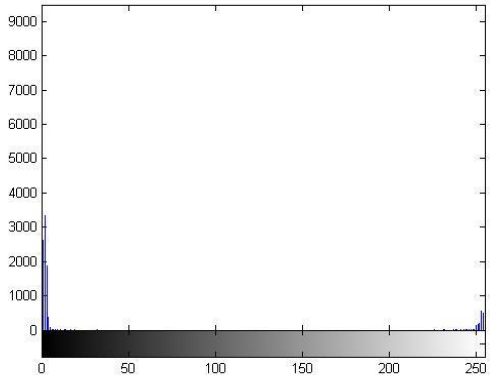

Fig-5.6 Histogram of above image after applied MFCC and pitch value to image

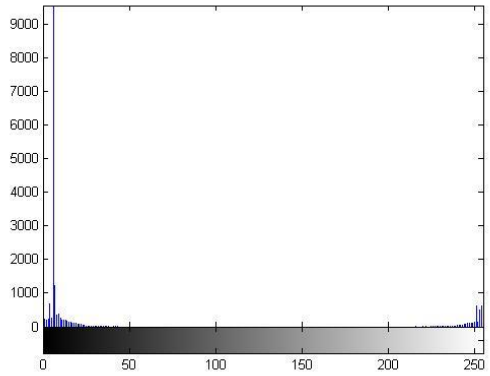

Fig-5.7 Histogram of Decrypted mage

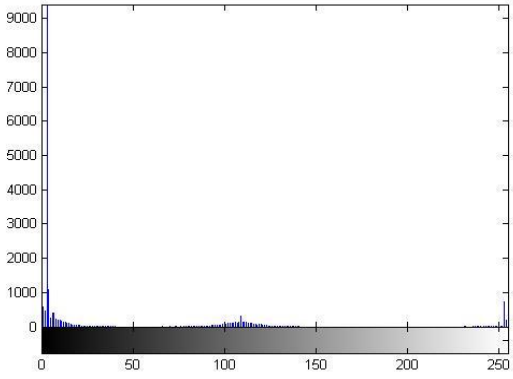

Fig-5.8 Histogram of Received Image after removing MFCC and Pitch

5.3 Conclusion & future work

Cryptography has a very great advantage in information security area that except of the expert no one can do harm to the information and securely we can transfer our confidential data to other party. Elliptic Curve Cryptography is a new technology which came in existence since 1965 by Koblitz [10] and miller. A large number of researches is going on ECC but ECC great advantage is its smaller key size compare to other algorithms such as DES (Data Encryption Standard) and RSA (Rivest- Shamir- Adelman). ECC works on small device in a better way compare to huge machines, ECC works on those device which are in constrained environment or use resources in a limit. We can make use of MFCC in making Elliptic curve digital signature through MFCC coefficients and we also can make Elliptic Curve Cryptography Digital certificate Through MFCC. These certificates can also be used further by the third party and also used by many users in different-2 encryption algorithm.

Future work related to decrypted image and image recovered after removing the MFCC coefficients from image, we can further perform image enhancement techniques such as histogram equalization and contrast stretching and noise removal from an image. Further this image can be recovered in a better way by applying the digital image processing [12]. Further if we analyze the histogram of the each image then one by one histogram of the original image and decrypted image is approximately same. Drawback is exactly we are not getting original image but further we can also do many operation with received image for improvement

Proposed approach in this paper works better for satellite images and can better work for text data and further we can also us MFCC coefficients in other encryption algorithm because it is the unique feature from human characteristics and freely available from every user. Here we mean to say each individual can use their voice for authentication of the data and this is more secure in public network. Generally in biometrics speech is available easily and also can detect and synthesized in any condition and in any environment but there is a drawback i.e., noise. If your recording of voice is in noisy environment then it will be a little bit more complex to detect easily the data. With use of speech user need not required keyboard but recording device quality

must be better in recording manner. Furthermore work is going on speech processing. We are also just improving our implementation in better way

References

[1] William Stallings, "Cryptography & Network Security", Printce Hall, 5th Edition.

[2] Alessandro Cilardo, Luigi coppolino, Nicola Mazocca, and Luigi Roman, "Elliptical Curve Cryptography Engineering", Proceedings of the IEEE, vol. 94, no 9, pp. 395-406, Feb. 2006 .

[3]"SpeechProcessing",dea.brunel.ac.uk/cmsp/home…/chapter13-speech%20processing.pdf.

[4] en.wikipedia.org/wiki/Speech_processing.

[5] G. Khare, M. Kulkarni, "Generation of excitation signal in voice excited linear predictive coding using discrete cosine transform", TENCON 2005, IEEE region 10, page 1-4.

[6] S.S. Upadhyay , "Pitch detection in time and frequency domain", ICCICT 2012,IEEE, page 1-5.

[7] Adam J. Albirt, "Understanding & Applied Cryptography and Data Security" CRC press, Pearson.

[8] G. Malherpe, O. Mesde and H. Riz, "Acoustic synthesis and methodology for improving cochlear implant speech processing techniques", Proc. Of the 25th annual international conference of IEEE *EMBS,* 2003

[9] H.Nagahama, Y.Miyanaga and N.Ohtsuki, "An adaptive speech analysis for speech recognition system", Proc. Of IEEE ISPACS 1999, pp.745-748, Dec. 1999.

[10] N. Kolbitz, Elliptic Curve Cryptosystems, Mathematics of Computation, vol.48, 1987, pp.203-209.

[11] Certicom website http://www.certicom.com/index.php? action =ecc_tutorial, home.

[12] Rafael C. Gonzalez, "Digital Image Processing", Third Edition.

[13] http://en.wikipedia.org/wiki/Mel_scale

[14] http://en.wikipedia.org/wiki/FFT

[15] H. Teffahi, "Relationship between control parameters and outputs in the two mass model of vocal cords", ICMCS , 2011 IEEE page 1-5.

[16] H.Hoge "A parametric representation of short time power spectrum based on the acoustic properties of the ear", ICASSP 1984, speech and signal processing page 49-51.

[17] Satellite Imagery https:// en.wikipedia.org/wiki/Satellite_imagery

[18] Uses of Satellite Images wp.cedha.net/wp.../The-uses-of-satellite-imagery-Taillant-Picolotti.pdf

[19] http://en.wikipedia.org/wiki/DES

[20] http://en.wikipedia.org/wiki/Asymmetric_key_cryptography

[21] http://en.wikipedia.org/wiki/RSA