Image Authentication and Security using Digital Signatures

A thesis submitted towards the fulfilment of requirement for the award of the degree of

Master of Engineering

In

Wireless Communication

Submitted by:

Harpreet Kaur

Roll No: 801463010

Under the Guidance of:

Dr. Ajay Kakkar

Assistant Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

(Established under the section 3 of UGC Act, 1956)

PATIALA – 147004 (PUNJAB)

JUNE 2016

CERTIFICATE

Certified that the thesis entitled ***"Image Authentication and Security using Digital Signatures"*** being submitted by **Ms. Harpreet Kaur** to the **Department of Electronics and Communication Engineering, Thapar University, Patiala** in the fulfilment of the requirements for the award of the degree of **"Master of Engineering"** is a record of bona fide research work carried out by her. She has worked under my guidance and supervision and fulfilled the requirements for the submission of this thesis which has reached the requisite standard. The matter presented in this thesis does not incorporate any material previously published or written by any other person except where due reference is made in the text.

The results contained in this thesis have not been submitted in part or full to any other institute or university for the award of degree or diploma.

Dr. Ajay Kakkar
Assistant Professor,
Department of ECE,
Thapar University,
Patiala (P.B) – 147004
India

Scanned by CamScanner

DECLARATION

I hereby declare that the thesis report entitled **"Image Authentication and Security using Digital Signatures"** is an authentic record of my study carried out as requirement for the award of degree of ME (Wireless Communication) at Thapar University, Patiala, under the supervision of **Dr. Ajay Kakkar**, "Electronics and Communication Engineering Department" during master's degree.

The matter presented in this dissertation has not been submitted to any other University/Institute for the award of any other degree.

Harpreet Kaur

Date: 13/7/16

Harpreet Kaur
Roll No-801463010

This is to certify that the above statement made by the student is correct to the best of my knowledge and belief.

Date: 14/7/16

Dr. Ajay Kakkar
Assistant Professor, ECED

Countersigned by:

Dr. Sanjay Sharma
Professor and Head, ECED
Thapar University, Patiala

Dr. S.S. Bhatia
Dean of Academic Affairs
Thapar University, Patiala

Scanned by CamScanner

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr. Ajay Kakkar, Assistant Professor,** Electronics and Communication Engineering Department, Thapar University Patiala for his patient guidance and support throughout this report. I am truly very fortunate to have the opportunity to work with him. I found his guidance to be extremely valuable. I am also thankful to our Head of Department, **Prof. Dr. Sanjay Sharma** and P.G. Coordinator, **Dr. Amit Kumar Kohli** and programme coordinator **Dr. Hem Dutt Joshi**. I would like to thank the entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Harpreet Kaur

Harpreet Kaur
ME-WC
801463010

Scanned by CamScanner

TABLE OF CONTENTS

Abstract

Data security is an essential component of an organization in order to keep the information safe from various competitors. It helps to ensure the privacy of a user from others. An unsecured channel becomes more vulnerable to the threats that can lead to data corruption, hacking or compromise of user's identity and privacy Hence, secured and timely transmission of data is always an important aspect for an organization. Current aspects of cryptography and need of data security in communication are discussed in the beginning of this thesis. It also covers the various digital techniques employed for the data security with their merits and demerits.

The work done by the various researchers in the field of cryptography has also been discussed. Observations from literature survey, problem formulation, objectives and research mythology has been formulated to design a new methodology. Proposed scheme meets the objectives such as less time consumption for signature generation and secure communication. After presenting the proposed schemes, their results and comparison with existing schemes of Yang and Kot, Tzeng and Tsai, Wu and Liu has been done on the basis of original data manipulation, bit length of signature generated, and compression supportability. Finally, it has been concluded that both the proposed schemes are well efficient in securing the image data with reduced signature length, also the advanced proposed scheme itself acts as encryption tool therefore, no separate encryption is required for additional security of image. Both the schemes works real fast and hence suitable for real time applications.

List of Abbreviations

GSM	Global System for Mobile
CDMA	Code Division Multiple Access
MAC	Message Authentication Codes
RDS	Remote Data Services
JTC	Joint Transform Correlator
FRR	False Rejection Ratio
FAR	False Acceptance Ratio
GPS	Global Positioning System
SHA	Secure Hash Algorithm
RFID	Radio Frequency Identification
GDC	Generalized Digital Certificate
DSA	Digital Signature Algorithm
RSA	Ron Rivest, Adi Shamir and Len Adelman
CED	Concurrent Error Detection
PKC	Public Key Cryptography
IBC	Identity Based Cryptosystem
KMC	Key Management Center
DTW	Dynamic Time Warping
ANN	Artificial Neural Network
BS	Blind Signatures
FV	Fuzzy Vault
BFS	Boosting Feature Selection
ABS	Attribute based Signature
GCD	Greatest Common Divisor
PPOFE	Privacy-Preserving Optimistic Fair Exchange
OFE	Optimistic Fair Exchange
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions

TLD	Top Level Domains
PGP	Pretty Good Privacy
PKI	Public Key Infra Structure
AES	Advance Encryption Standard
CA	Certificate Authority
ISO	International Organization for Standardization
ANSI	American National Standards Institutes
IEEE	Institute of Electrical and Electronics Engineers
EVS	Electronic Voting System
DLP	Discrete Logarithm Problem

List of Figures

LIST OF TABLES

CHAPTER 1
INTRODUCTION

This chapter describes the importance of data security of documents being transferred on a network along with the possible threats that can arise during transmission and their counter measures. A brief introduction of the need of digital signatures in cryptography, evolution from handwritten sign to digital sign, general steps to create a digital sign and key management for digital signature generation and authentication process has also been discussed.

1.1 ORIGIN OF CRYPTOGRAPHY

From ancient times, human being had two basic needs which are; (i) to communicate in order to share information, and (ii) selective communication. These two needs became necessity to create a coding method to provide secrecy while sharing the important information, therefore, only the authorized person can retrieve the original information [1]. The art and science of converting a message into unintelligible format to introduce secrecy and the coded message is able to reconverted back to its original form is known as “Cryptography”.

With the advent in the field of information technology over the last decade, new methods of transferring data with or without internet are enlarged [2]. All the paper work is stored in terms of softcopy that mean digital data is preferred over hard copies of same information in paper format. Banking, transport services and even government agencies prefer E-Commerce for interaction between them and end users like us. E-Commerce being a reliable and fast method for providing services and it is considered as one of the powerful way of communication [3]. The development in digital mobile networks such as GSM and CDMA along with the high speed internet services made it possible to access online services in one click.

The advantages of the digital systems are the reason behind the success of these technologies. Data integrity and quality is maintained to ensure the number of errors in digital system would be less [1]. Despite of the various advantages of digital systems, there are some liabilities alongside. Digital systems are complex and very hard to restore [4].

1.2 History Of Cryptography

The art of cryptography was started along with the art of writing. With the evolution in civilization, human being started to form tribes, groups and kingdoms to live. All this led to the ideas of power, battles, politics and supremacy, which gave rise to the need of people to secretly communicate with the selective recipient only [1]. This ensured the evolution of cryptography as well.

- **Hieroglyph – The Oldest Cryptographic Technique**

  Hieroglyph is the best known evidence that proves, cryptography is not new and it is part of our communication system from a long time. Some 4000 years ago, the Egyptians used this technique of hieroglyph to communicate [2]. Only the scribes who were used to transmit important messages on behalf of the kings, knows the secret code. Example of hieroglyph is shown in figure 1.1:

Figure 1.1: Example of "hieroglyph" by Egyptians [2]

- **Mono - Alphabetic Substitution Cipher**

  During the time of 500 to 600 BC, the scholars developed mono-alphabetic substitution ciphers, in which the original alphabet of message is replaced by other alphabet depending on the secret rule applied [1]. The secret rule became a key, without this, the recipient could not retrieve the original message.

- **Caesar Shift Cipher**

  This cipher method was developed by the Romans. In Caesar shift cipher, as the name

suggests, shifting of alphabets would be done. Mostly the alphabets of a message were shifted by an agreed number and only the authorized recipient knows this number, so back shifting of the letters of received message would be applied to get the information [2]. Example of Caesar shift cipher is given below:

ORIGINAL TEXT: M Y N A M E I S H A R P R E E T

Each letter is shifted by '3'

CYPHER TEXT: P B Q D P H L V K D U S U H H W

- **STEGANOGRAPHY**

The aim of steganography is not only to provide data secrecy but also to make sure that any unauthorized user or intruder gets no evidence of the existence of information. Example is invisible watermarking [1]. The intruder is unaware of the presence of hidden information where as in cryptography unauthorized user knows the information is being transferred, but one cannot decode the message without having the secret key used for message encryption [1]. Example of steganography is shown in figure 1.2.

(a) (b)

Figure 1.2: (a) carrier file and (b) carrier file with hidden message

1.3 EVOLUTION OF CRYPTOGRAPHY

During the European Renaissance from 14th to 17th century, various Papal and Italian states researched and invented the cryptographic techniques [2]. Various attach techniques were explored to break the secret codes.

- In 15th century, researchers and scholars improved the existing coding techniques and a new "Vigenere Coding" that allows movement of letters in the message with variable places instead of moving them at the same places, came into existence [3].
- After the 19th century, more sophisticated coding techniques were evolved from the previous cryptographic techniques that use ad hoc approaches for encryption [1].
- In early 20th century, Enigma rotor machines were launched for the very first time and that invention of electromechanical and mechanical research provided the more efficient and advanced means of coding the message [2].
- During the time period of World War II, cryptography and cryptanalysis became extremely mathematical.

With the development taking place in the field of cryptography, military units, government organizations and some other corporate houses also started adopting the various applications of cryptography [3]. Earlier, it was used to guard their secrets from unauthorized persons. Now, with the arrival of computers and fast internet services, it became possible to bring the effective cryptography within reach of common people.

1.4 MODERN CRYPTOGRAPHY

Modern cryptography uses the concepts of number theory, probability theory and computational-complexity theory in addition with the computer systems to provide efficient communication security [3]. Major characteristics of the modern theory are:

- It is applicable on binary bit sequences.
- It uses publicly known mathematical tools for coding of information and involves the usage of secret keys, without which it becomes almost impossible for a person to retrieve the original information, even if one has the information of coding scheme used

- It requires people who are interested in secured communication by acquiring the secret key only [1].

1.5 Context Of Cryptography

The study of cryptosystems is known as "Cryptology". It can be subdivided into following sub-branches:

- **Cryptography**

  The art and science of making cryptosystems that are capable of providing information security is known as cryptography [4]. It uses mathematical tools or algorithms to provide fundamental information security. It deals with securing of digital data from known and unknown threats.

- **Cryptanalysis**

  It is the art and science of cracking a cipher text or it is the study of various cryptographic mechanisms with intension to break them [5]. Cryptography and cryptanalysis both co-exists. It is also used for the security testing of a cryptographic scheme.

1.6 Goals Of Cryptography

Cryptography provides many benefits in the field of information security. The main aim of a cryptographic technique at the time of its designing is, it to achieve the following most essential services to provide data security.

- **Confidentiality**

  It is the fundamental security service offered by cryptography. It is responsible to maintain the privacy and to prevent an unauthorized access by any means [3]. It could be achieved through various methods such as physical securing or mathematical algorithms for data encryption.

- **Data Integrity**

  This service identifies any alteration to the data. The data may get modified accidently, during the transmission or intentionally by an unauthorized user [2]. It cannot prevent the alterations but it provides a means to detect whether the data is intact or not.

- **AUTHENTICATION**

  This service deals with the identification of the users present in a network. It confirms that whether the received data is actually sent by an authorized user or not [1]. It can have two variants:

  a) **Message authentication:** It verifies the identity of message sender without considering the route or system through which the message has reached its destination.

  b) **Entity authentication:** It gives the assurance that a specific registered entity has sent the message; say a particular website [2].

- **NON REPUDIATION**

  It is a security service to ensure that the original sender of data cannot deny the ownership or transmission of the said data to its recipient or third party. It is the most desirable property in situations where chances of a dispute are high over the exchange of data [3]. Such as, after electronically placing an order through the internet, a purchaser cannot refuse the purchase order, if and only if non-repudiation service was activated prior to the transaction.

1.7 CRYPTOGRAPHIC STANDARDS

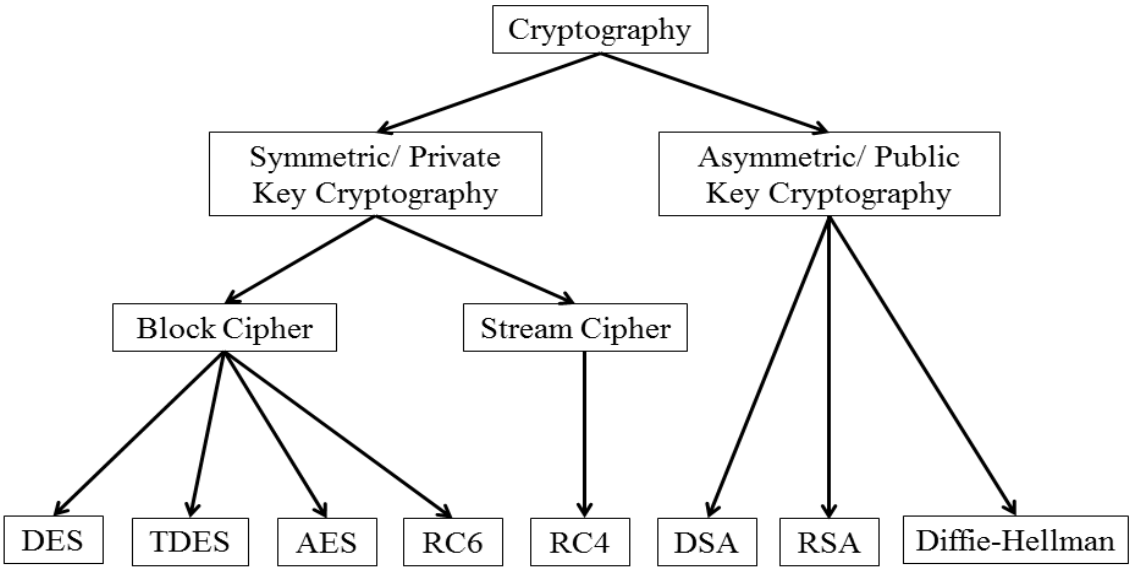


Figure 1.3: Taxonomy of cryptographic standards

There are a large number of cryptographic techniques that are available to achieve data secrecy. But only some of these algorithms became standards and the list of these standards is shown in figure 1.3.

- **SYMMETRIC OR PRIVATE KEY CRYPTOGRAPHY**

  It is the cryptographic algorithm in which the encryption key, denoted by e and decryption key, denoted by d are identical or they may be transformed from each other by least computational complexity. In most of the cases keys used to encrypt and decrypt a message are same and the key is known as secret key which is shared among two or more parties. The only difficulty of using symmetric key is to share the secret key through a safe channel [5].

- **ASYMMETRIC OR PUBLIC KEY CRYPTOGRAPHY**

  This algorithm comprises of a pair of keys known as private and public key pair. A certificate authority generates the private key along with its matching public key. As the name suggests, the pubic key is made available to anyone who wants to share a piece of information with the intended recipient, whereas the private key remains secret and is only known to the owner of that key [5]. Any message which is encrypted by applying the public key can be decrypted by using its matching private key only and reverse is also true.

- **BLOCK CIPHER**

  It is a method of encrypting plaintext into cyphertext by first dividing the plaintext into fixed length blocks (64 bits in one block) and then these blocks are encrypted one at a time [4] .

  It is the easiest way to encipher a plaintext when the message length exceeds the desired block length. Initially, the whole message is breaked down into n bit block length and then each block is encrypted individually as shown in figure 1.4.

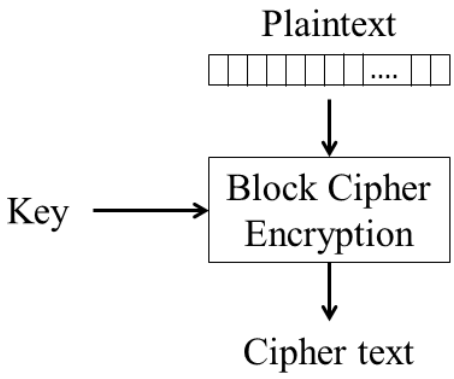


Figure 1.4: Block Cipher generation process

If an n-bit plaintext is lesser in length than the block size, it is usually padded such that it becomes equal the block size and is ready to be encrypted. Since, all the block ciphers are symmetrical; therefore, the inverse of encryption algorithm will result in original plaintext.

- **STREAM CIPHER**

  It is an alternative of block cipher, to eliminate the error propagation problem of identical blocks in block cipher. In stream cipher, the cipher text of the pevious encrypted block is commonly applied to the next block, so that, identical blocks encrypted by this algorithm do not produce the same block cipher [4].

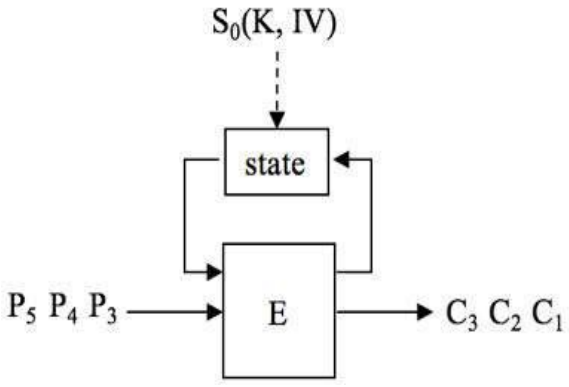


Figure 1.5: Stream Cipher Mode

In stream cipher, the plaintext or message is processed one bit at a time and then encrypted. The whole process continues till the complete message gets encrypted

according to the internal state and is controlled by key K, public Initialization Value (IV). In figure 1.5, P_i and C_i represents the plaintext and cipher text respectively [5].

1.8 HASH FUNCTIONS

It is a function which takes a variable length string as an input message and returns a static length alphanumeric string that is also known as hash value, message digest, digital fingerprint or checksum [4]. It doesn't require any key for its functioning. It is applicable for message integrity checks, authentication, digital signatures and various information security applications.

1.9 CRYPTOGRAPHY PRIMITIVES

Cryptography primitives are the tools and techniques that can be selectively used to provide the desired set of security services (i) Encryption, (ii) Message Authentication Codes (MAC), (iii) Hash Functions, and (iv) Digital Signatures.

Table 1.1: Cryptographic primitives and the security services they offer.

Primitives / **Services**	**Encryption**	**MAC**	**Hash Function**	**Digital Signature**
Confidentiality	Yes	No	No	No
Data Integrity	No	Yes	Sometimes	Yes
Authentication	No	Yes	No	Yes
Non-Repudiation	No	Sometimes	No	Yes

Table 1.1 shows the security services that these primitives can achieve on their own. Cryptography primitives are related to each other and used in combinations to achieve a desired level of security from a cryptosystem [5].

1.10 NEED AND IMPORTANCE OF DIGITAL SIGNATURES

The potential sources of attacks are increasing due to the rapid increase in internet connections as more users are getting connected globally. Eavesdropping critical data and

trespassing security limits of someone has increased since the past few years.

Rapid growth of wireless networks and communication systems made it even more difficult to manage the integrity, quality and security of information being transferred [4]. Hence, the result is increased cyber-crime, viruses etc. All this arise the need of more secure and reliable network that can deal with such attacks and it can only be possible through cryptographic primitives. Digital signatures are best suited to achieve the basic services that are data integrity, authentication and non-repudiation. Digital signature combined with encryption becomes more effective to attain confidentiality.

1.11 DIGITAL SIGNATURE

Digital signatures are best appropriate to achieve authentication, data integrity and cannot be forged easily. Handwritten signatures are used to authenticate the paper based documents, while digital signatures are used to bind a person or entity to the digital data. Digital data can be government documents. [5]. This signature can be independently verified at the receiving end by receiver as or any third party.

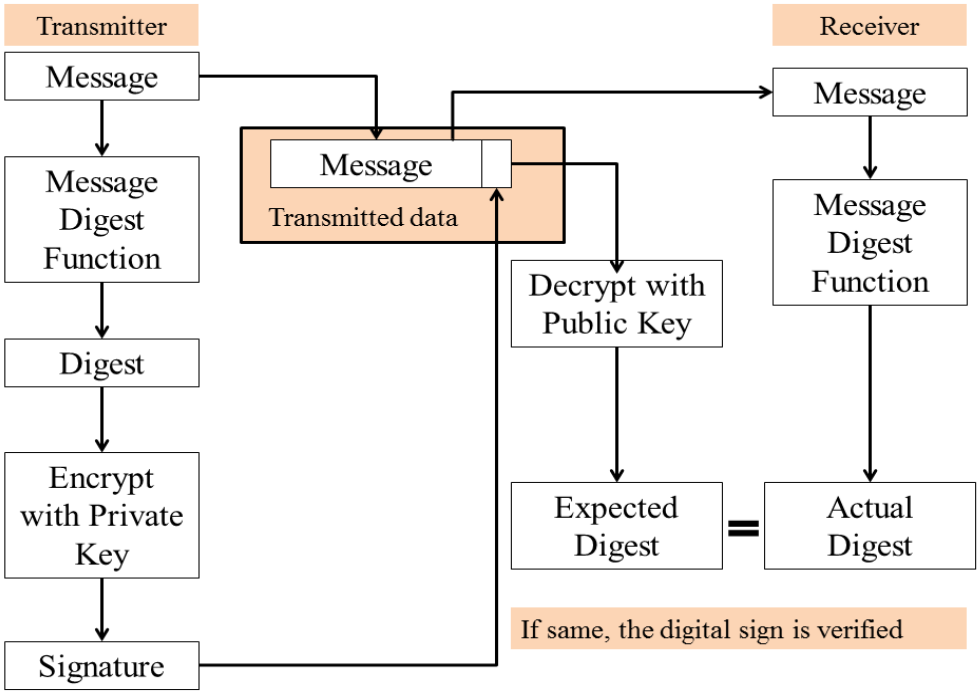


Figure 1.6: Digital Signature process flow

The main purpose of digital sign is not only restricted to authenticate the document through signing it but also to detect the undesired changes at the receiving end that may have occurred during its transmission. Digital signatures are generated from the input data and the private key of the signer. If original data gets manipulated, receiver can easily verify it by matching the received digital sign with the sign computed for received data using the matching public key of signer, hence one can check the integrity of signed data [5]. Working of digital signatures is described in figure 1.6.

The digital signing process can be sub-divided into following parts:

- **SIGNATURE GENERATION**

  In order to sign the message data, sender has to create a message digest by extracting some of the features of message that can be achieved with the help of message digest function. The sender must have his own valid pair of private and public keys [4]. Once the message digest is generated, the sender will encrypt it using his private key and the signature obtained from above process will be attached to the message before its transmission.

- **SIGNATURE VERIFICATION**

  The receiver will detach the attached signature and information message from the received data and will obtain the expected digest by decrypting the received sign using his public key. Receiver will also generate a new message digest of the received data by utilizing the same digest function [5]. If both the message digests comes out to be same, the sender will be marked as authentic in such case.

1.12 APPLICATIONS OF DIGITAL SIGNATURES

Digital signatures have the greatest impact on commerce after the invention of money. Digital signatures allows the signing and verifying authorities to identify the signer and make real time commitments in cyberspace in same way as it is being done in actual space [5]. Applications of digital signatures are as follows:

- Initial use of digital signatures is limited to the applications where long-term archival is not so important, for example purchase orders, authentication to on-line services, electronic funds transfer etc.
- Applications requiring long-term archival such as birth and death certificates, government records etc. will require the improvement in electronic data archival centres to make them capable of verifying digital signatures and associating with the identity of signer [5].

1.13 ORGANIZATION OF THE THESIS

In this thesis, starting from the basics of cryptography through the advancements in the field of digital signature is discussed. The aim of this thesis was to study various algorithms provided already in literature and then to design an approach that can be easier to operate yet more secure and easier to implement. There is a proposed digital signature algorithm which drives the thesis and is discussed in detail in chapters 4 and 5. Following is the outline of this thesis and the main contribution of each chapter:

- In Chapter 1, a brief introduction of data security and digital signature has been discussed along with the basics of these and the terminology involved. The outline of thesis has also been drawn.
- In Chapter 2, work done by various researchers has been studied to observe best possibilities; so as to find the gaps in studies and then to draw the problem formation. This section mentions some of the relevant papers that helped in achieving the targeted results.
- In Chapter 3, critical analysis of various digital signature schemes has been done. Further, taken into account is the process of replacement of traditional digital signature schemes by more efficient, secure and fast algorithms.
- In Chapter 4, the proposed work has been discussed. A modified digital signature scheme has been developed and all the necessary steps along the path followed are shown in this chapter. Finally the key parameters on which the proposed algorithm works has been discussed. Extended version of the proposed methodology has also been mentioned.

- In Chapter 5, the simulation results of proposed approach and its comparison with existing schemes of Yang and Kot, Tzeng and Tsai, Wu and Liu has been done on the basis of original data manipulation, bit length of signature generated, and compression supportability .
- In Chapter 6, the concluding remarks of the proposed work and the scope for the future work have been discussed.

CHAPTER 2
LITERATURE REVIEW

In this chapter, work done by various researchers to achieve better cryptographic algorithm for secure communication has been provided. The aim of this section is to point out the advantages of various data security systems and to look for the areas where development can be possible to make the system more reliable. Observations and conclusions have also been drawn. Finally, problem formation has been discussed and objectives are determined.

Marc S. *et al.* [6] designed an algorithm that uses digital signatures to provide continuous image authentication and could also support some image formatting techniques like lossy compression. It introduced the concept of generating the signature from the features of the image. Detection of set of features that could be applicable for signature generation was also discussed. The problem with this scheme is that the signature embedded in image and hence the contents of original image get changed. This scheme could be extended to implement it for video sequences.

Ping W. W. *et al.* [7] introduced an image watermarking scheme in which the watermark or hash generated from the image was embedded into the original image and only the authorized user could regenerate the image by applying its own key. Any changes in image data would be represented by errors in watermark. This scheme helps in preventing the forgery of image data, as if correct key is not used to extract the watermark, it will result an image showing random noise.

Ching-Yung L. *et al.* [8] designed a robust digital signature based image authentication scheme that was capable to distinguish between tampering and lossy compression. The trustworthiness and integrity of the multimedia data was retained by discarding any malicious manipulations and allowing some desired changes that might had occurred due to lossy compression techniques, or inability of the devices used. The work could be extended by using RDS based on different transcoding applications for video authentication.

Aloka S. *et al.* [9] built a new image encryption technique for secure transmission. Coding technique was Bose-Chaudhuri Hochquenghem and authentication was achieved by adding the digital signature to the encoded image format. At receiver either JTC or digital correlation technique or the Vander Lugt geometry could be used to validate the sender by extracting the digital signature.

Chun–Shien L. *et al.* [10] presented a structural digital signature based approach that uses the image data in wavelet transform domain to construct the signature. The approach was well capable to distinguish between content preserving changes and content changing modifications. However, the scheme can be easily fooled, if parent child pairs are known to the attacker and its coefficients can be manipulated in such a way that the system cannot identify its forgery.

Min W. *et al.* [11] worked on data hiding techniques for embedding of data such as scanned text, signatures and figures in binary images. Data was embedded into the image such that it creates no noticeable artifacts. Registration marks were utilized for extraction of hidden data without the use of original image.

Mehmet U. C. *et al.* [12] designed a new watermarking technique that was well capable to validate the sender before the recovery of original image. Hence, it saves the computational time in cases where sender validation fails or the reconstruction is not required. The features like computational efficiency, public/private key support and improved tamper-localization accuracy make it well suitable for practical applications.

Huijuan Y. *et al.* [13] proposed a binary data hiding scheme for binary image authentication. The methods to locate the embeddable pixels in a block for a variety of different block schemes were also provided. The small block size of 3x3 makes computational time large. The invariant features of the proposed data hiding process makes it less complex and free from the side information requirements.

Francesco B. *et al.* [14] worked on to find a cheap practical technique which was feasible and efficient to mitigate the vulnerability of digital signature because that vulnerability allows the attacker to sign documents and to exploit them without any intention of signature's owner. The complexity of the approach is very high, but the nice feature of this approach is that it relies on the usage of Java cards instead of firmware-only-programmable smart cards.

Julita A. *et al.* [15] worked on online signature verification which was a process of verifying the writer's identity by using signature verification system. The tight security that this software offered, would indirectly contribute towards the increased FRR but manage to lower down the FAR where forgery signatures can be hardly verified as genuine signatures.

S.M.Saad *et al.* [16] researched on multi-scale features for image authentication and constructed an improved version of digital signatures using multi-scale features and key dependent parametric wavelet filters. This scheme is well suitable for real time applications over wireless media because of its less computational overheads. The only problem with using wavelets is their high computational complexity and low security.

Panagiota L. *et al.* [17] worked on to evaluate the provision of non-repudiation in electronic transactions. To evaluate the provision of non-repudiation, two technological methods were compared: a) digital signatures and b) biometrics. Non repudiation is required in many existing applications such as e-commerce, e-banking, and e-governance and its successful provision could lead to the development and enhancement in digital contract signing, access to confidential documents and applications, registration in several activities.

M. O'Neill *et al.* [18] worked on a low-cost GPS digital signature architecture, which was a combination of an optimized GPS algorithm design and an optimized SHA-1 design for low-cost RFID tags. The proposed architecture could be used for device authentication to prevent tag cloning and to provide data authentication to prevent transmission forgery. The design offers significant improvements over previous work on RFID digital signature architectures in terms of area, power, and timing.

Lein H. *et al.* [19] worked on the concept of Generalized Digital Certificate (GDC) that can be used to provide user authentication and key agreement. A GDC contains user's public information, such as the information of user's digital driver's licenses, the information of a digital birth certificate, etc., and a digital signature of the public information signed by a trusted CA. The key management in purposed GDC is much simpler than using public-key digital certificate but the scheme is very time consuming.

Nadia M.G. *et al.* [20] worked on a novel digital signature protocol that was based on the iterated function system attractor, which was regarded as an emerging method. The attractor was used in the encryption and decryption of a hash function to ensure the protection of the document from eavesdropping and integrity during the transmission. The novel scheme utilizes the inherent advantages of a fractal attractor in terms of smaller key size and lower computational overhead compared with its counterpart public cryptosystems, such as the DSA and RSA.

Yao-Chung L. *et al.* [21] worked on distributed source coding technique to use Slepian-Wolf coded quantized image as authentication data to enhance the system robustness and security. The localization decoder used sum-product algorithm for tampering localization and decodes the Slepian-Wolf bit stream that gave the relationship among projections of original image, target image and the block states. To achieve zero rate of falsely deemed tampered blocks, the rate of undetected tampered pixels become about 2%.

Che-Wei L. *et al.* [22] built a Shamir secret sharing based image authentication scheme that was capable to repair data for greyscale images. Multiple shares consisting of authentication signals for each block were generated using Shamir secret sharing scheme and sent along with the original greyscale image in PNG format. Reverse Shamir scheme was implemented at receiver for tampering localization and image authentication. Other block sizes could be included with related parameters such as number of authentication signal bits and coefficients for secret sharing, etc for further improvement.

Kun Ma *et al.* [23] worked on a novel Concurrent Error Detection (CED) scheme to counter fault-based attack against RSA by exploiting its multiplicative homomorphism property. In order to achieve high performance, the CED technique requires successive messages to share the key. It offers several advantages, including strong resistance to fault attacks and small time overhead.

Sebastiano B. *et al.* [24] proposed an image hash component based image alignment method for tampering localization in distributed forensic systems. Spatial distribution of image features was encoded by image hash to deal with textured and contrasted tampering patterns. The work could be extended by analyzing the work in depth to achieve more accurate estimation of the geometric transformations.

Shiva M. G. *et al.* [25] worked on a secure node disjoint multipath routing protocol for wireless sensor networks. The data packets were transmitted in a secure manner using the digital signature crypto system. It was compared with an adhoc on-demand multipath distance vector routing protocol. It shows better results in terms of packet delivery fraction, energy consumption, and end to end delay compared to the adhoc on-demand multipath distance vector routing.

Ajay K. *et al.* [26] worked on a new approach for generating keys from the available data. The model takes minimum time to replace the faulty keys with the fresh keys. The security also increases, if the key size is increased and the key shifting time (δ) is reduced; the above combination may be adopted for secure transmission.

Andrew C. C. Y. *et al.* [27] worked on a new variant of the Fiat–Shamir transformation for digital signatures, referred to as transformation. In particular, it is shown that the signatures for Discrete Logarithm Problem (DLP) developed, in essence, the advantages of both Schnorr's signature and the digital signature standard (DSS), while saving from the disadvantages of them both.

Erfaneh N. *et al.* [28] worked on the analysis of the security systems and the emphasis was on digital signature, hashed message algorithm. The algorithm introduced a novel technique for producing small-sized output of digital signature as a result; the new scheme is potentially practical: signing and verifying signatures are reasonably fast, and both speed and time are improved.

SK Hafizul Islam *et al.* [29] worked on a provably secured certificate-less digital signature scheme using elliptic curve cryptography. Hence, the certificate-less public key cryptosystem removes the complex certificate management procedure and the private key escrow problem of traditional PKC and Identity Based Cryptosystem (IBC). The proposed scheme is more efficient than IBC and PKC based signatures.

Manjot B. *et al.* [30] worked on a protocol to securely transfer the group key. The KMC carefully hides the password or key in user's image without making any visible differences between original image and stego image. Simulation tools used were Java and MATLAB. The confidentiality and security of key depends on steganography. The work could be extended by incorporating the member join and leave feature with more security.

William S. *et al.* [31] worked on three digital signature algorithms that were approved by the national institute of standards and technology and which have also been standardized by a number of other organizations, including ISO, ANSI, and IEEE. Two additional digital signature algorithms are also discussed.

S. Rashidi *et al.* [32] worked on an effective method for online signature verification. The aims of the work were to study two problems: a) Comparison of functional features from the viewpoint of consistency, and b) discrimination between genuine and forgery signatures, possible improvement in Dynamic Time Warping (DTW) distance computation. Further improvement would include detail study of DTW for an optimal distance finding method. This system perhaps could perform better in the verification phase.

Othman O. khalifa *et al.* [33] worked on an offline signature verification schemes which considered as a highly secured technique to recognize the genuine person's identity. It addresses the offline signature verification technique using Artificial Neural Network (ANN) approach. The main benefit of using offline systems is identifying the right person and providing secure services.

Kazi Md. R. A. *et al.* [34] presented a comparison between two blind signatures (BS), it ensures the confidentiality of the private information of a user. The comparison of computation time requirement showed that Hwang et al.'s scheme [76] requires much time than Chaum's scheme [77] to conduct the simulation. However, Hwang et al.'s scheme is certainly admired. The reason is that it fully satisfies all the requirements of an ideal BS scheme.

Angela P. *et al.* [35] introduced a scalable fragile watermarking approach for authentication of scalable compressed images. The scaled image resolution and quality did not produce any false alarm, hence the approach could identify the tampering of data and protects the image from mark transfer and collage attacks.

Rouzbeh B. *et al.* [36] proposed a new scheme which was more efficient in comparison to Duan's scheme [78]. This scheme offered more efficient confirmation and disavowal protocols for both the signer and the verifier. It results in better efficiency in signature generation, proof generation and verification compared to the scheme proposed by Duan.

Ashok K. B. *et al.* [37] introduced a new online signature based cryptosystem. This uses the Fuzzy Vault (FV) scheme to bind the key with biometric template, such that it becomes infeasible to access the secret key without the knowledge of biometric data. This scheme was simulated using MATLAB. The simulation result showed that the scheme was well secured with a FAR and FRR of 2.22% and 17.78% respectively and should be improved in future.

G. S. Eskander *et al.* [38] introduced an offline signature based FV system that uses two step Boosting Feature Selection (BFS) procedure for selecting user specific features. It achieves

97% FV recognition accuracy with system entropy of about 45 bits. The main limitation of this approach is that the two step BFS is most time consuming technique like it took 2 days for population based BFS. The parallel processing based FV decoders could be designed to reduce the decoding complexity.

Tatsuaki O. *et al.* [39] designed an Attribute based Signature (ABS) scheme. It supports non-monotone predicates which were earlier not presented in the existing fully secured ABS schemes. As a result the proposed scheme is comparable in efficiency to that of the most efficient ABS scheme in generic group model. However, this scheme is fully secured under standard assumptions only.

Xinyi H. *et al.* [40] presented a secured generic multi-factor authentication protocol to speed up the whole authentication process. Another authentication mechanism, named as stand-alone authentication, could authenticate users when the connection to the central server is down. In comparison with other generic design of multifactor authentication their design provides significant improvements in computation and communication.

Andrey L. *et al.* [41] proposes to use RFID technology to combine functions of physical access control, computer's access control and digital signature systems. This combination allowed to drastically increasing system's security. The high-end RFID tags with cryptographic possibilities and slight modification of digital signature calculation procedure make it possible to prevent obtaining digital signatures for fraudulent documents.

Gianluca L *et al.* [42] worked on the vulnerabilities of digital signature deriving from the "un-observability" of electronic documents. Possible mechanisms to contrast such vulnerabilities were also proposed, highlighting their positive and negative points under a perspective that does not ignore both practical and regulatory aspects.

Xu L. *et al.* [43] designed a new image authentication system based on the fixed point theory. The transform was selected on the basis of fragility, easiness of calculations and transparency

based on the GCD transform. Fixed point image of original image was generated from the selected transform and would be used for integrity check at the receiving end.

Gwoboa h. [44] proposed the simultaneous generation of $k, k-1 \, mod \, q$, so that the time required to generate a digital signature could be reduced. Using this method one can speed up the generation process of RSA key pair and blind RSA signatures. The security level of DSA remains same after applying this technique.

Qiong H. *et al.* [45] built a new scheme called Privacy-Preserving Optimistic Fair Exchange (P^2OFE). In OFE the major problem was that the semi trusted party got to know their full signatures as well. In the scheme, the arbitrator returns an intermediate value to the verifier and runs it to get actual signature. As a result, the overall security of the system was improved and even after the resolution of a dispute the arbitrator don't have the original signature or any evidence about an exchange between the parties.

Mohamed F. H. *et al.* [46] presented a key generation algorithm which exploits the property of chaotic signals over frequency selective fading channels. Chaotic signals are non-periodic this results in uncorrelated key bits, which improves the security of this algorithm. Another advantage of this algorithm is that irrespective of the channel coherence time, the algorithm can be well suitable for static or time varying fading channels. Initial values of chaotic generator could be exchanged to improve the security.

M. H. Jalalzai *et al.* [47] analysed the existing DNS challenges and the best solutions to deploy these challenges had been proposed. Security extensions of digital signatures were implemented to offer security to overall internet by providing DNS data authentication and end to end encryption for making a chain of trust in domains to avoid forgery. It requires precised approach with proper planning and skilful DNS administration for deploying and managing DNSSEC. TLDs domains are still not signed with DNSSEC; therefore, to form global chain of trust; it requires more enhancements in DNSSEC.

2.1 OBSERVATIONS FROM THE LITERATURE REVIEW

From the work done by the various researchers in the field of data security, following observations have been drawn:

- Some of the digital signature algorithm takes more time to execute; therefore, not applicable for real time applications. Some of the algorithms do not provide robustness of digital signatures.
- Counter measures are not efficient to provide a high level of security. If the number of users or data size increases with key length remains same, the security level surely increases. If propagation time is lesser than hacking time then our system is secure.
- Key is not transmitted; it is generated at the receiver. As there is no secured channel to send the key. This is known as key escrow therefore key must be generated at both sides from the available data.

2.2 PROBLEM FORMATION

Based upon the above observations, it has been concluded that there is a need to optimize the encryption system which takes less time to encrypt the data. From the above observations it has been concluded that

- There is a need to develop a cryptographic model in which keys are generated from the available data and should provide the flexibility to select short and long data length sequences as per the requirement. The selection of keys and round functions must be based upon the data sequence in order to reduce the hacking and processing times.
- The processing time is the function of the hardware used and it can be reduced by reducing the logical effort of a device. `It can also be controlled by selecting the optimized combination of data and key lengths.

2.3 OBJECTIVES

Finally, from the previous section, objectives have been drawn and are as follows:

- To study the various security aspects in digital signature.

- To optimize the bandwidth utilization in order to reduce the overheads on digital signature.
- To evaluate the signature generation time for various images of different sizes with optimized hash length.
- To compare the proposed scheme with existing schemes.

CHAPTER 3

DIGITAL SIGNATURES

The most important development in public cryptosystem is in the field of digital signature. It provides a set of security checks for the digital data that would be challenging to implement in any other way. In this chapter, evolution of digital signatures from the classical cryptosystems or basic cryptographic tools has been discussed. A brief introduction of digital signatures and how they work in practical applications and the legal value of digital signatures is discussed. It also describes the various encryption techniques for digital signatures such as RSA signature scheme, Feige-Fiat-Shamir signature scheme, Digital Signature Algorithm (DSA) and many more.

3.1 CLASSICAL CRYPTOSYSTEMS

The main goal of cryptography is to achieve privacy: two parties sender S and receiver R want to communicate secretly such that no adversary can know anything about what was communicated. A standard solution to this problem is classical cryptosystem or symmetric cryptosystems. In symmetric cryptosystem, the decryption key can be calculated from encryption key and vice-versa. In most of the cases, both keys are same that means a single secret key serves as encryption and decryption key. These cryptosystems are also known as single key cryptosystems, secret key cryptosystems and require that both the sender and receiver agrees on a key before the communication starts [48]. The security of symmetric cryptosystems lies in the key, as long as the key remains secret, the communication remain secret. Block representation of symmetric cryptosystem is shown in figure 3.1.

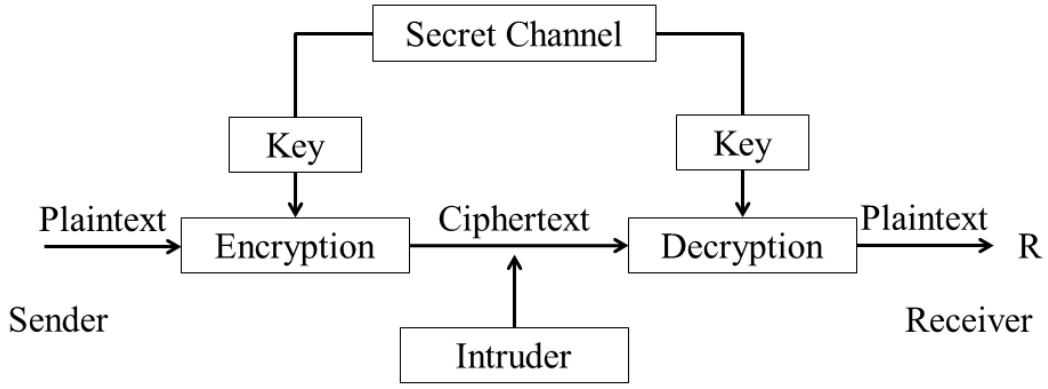


Figure 3.1: Classical Cryptosystem

Classical cryptosystem consists of the following:

- A plaintext space $\boldsymbol{P}$**:** It consists of all possible plaintexts $\boldsymbol{P}$.
- A cipher-text space $\boldsymbol{C}$**:** It consists of all possible crypto-texts $\boldsymbol{C}$.
- A key space $\boldsymbol{K}$**:** K determines an encryption algorithm $\boldsymbol{E_K}$ and a decryption algorithm $\boldsymbol{D_K}$ such that

$$D_K(E_K(P)) = P \qquad ; \text{P} \in \boldsymbol{P} \tag{3.1}$$

It is safe to send encrypted message using symmetric cryptosystem as it assures that an interception is unlikely to be able to decrypt the message [49]. However, with these advantages there are some disadvantages or problems of symmetric cryptosystem that are as follows:

- Secret key must be shared among sender and receiver before the encryption procedure starts.
- This sharing of secret key requires a completely secure channel, which is practically unlikely to find. If such channel exists then there would not be any need of symmetric cryptosystem for a communication.
- Key management is the most difficult part of classical cryptosystem. Each pair of users requires their own exclusive secret key [50]. Therefore for $\boldsymbol{n}$ users, number of secret keys required will be:

$$No.\ of\ \ keys\ \ required = \frac{n \times (n-1)}{2} \tag{3.2}$$

The key management of six users A, B, C, D, E and F is shown in the figure 3.2.

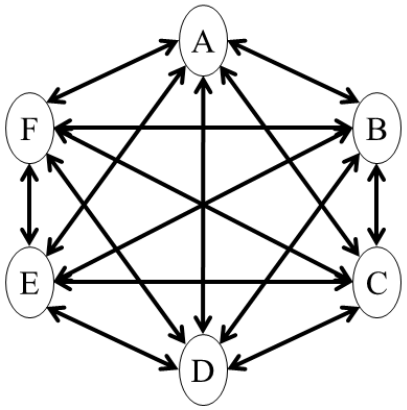


Figure 3.2: Key management in classical cryptosystem

- Symmetric cryptosystems are unable to deal the dispute between sender and receiver, which means a third party cannot identify the sender of a message. Because the key is common and receiver has the ability to generate any cipher-text that could have been generated by the sender.
- Authentication and message integrity can be successfully achieved by classic cryptosystems, but no one other than the receiving party can check the message authenticity and integrity of the message.

3.2 PUBLIC KEY CRYPTOSYSTEMS

In 1976, Whitefield Diffie and Martin Hellman proposed a new cryptosystem that becomes the ultimate solution to the above mentioned problems of classical cryptosystem and problems of key management in digital signatures. This new type of cryptosystem is known as Public Key Cryptosystem (PKC) [51]. A public key cryptosystem is a pair of $\boldsymbol{E_K}$ and $\boldsymbol{D_K}$, K belongs to key space $\boldsymbol{K}$ representing invertible transformations

$$E_K : P \to C \text{ and } D_K : C \to P \tag{3.3}$$

- For each K, $\boldsymbol{E_K}$ is inverse of $\boldsymbol{D_K}$.
- For each K, it is easy to compute both $\boldsymbol{E_K}$ and $\boldsymbol{D_K}$.
- For almost all K, each easily computed algorithm result equivalent to $\boldsymbol{D_K}$ is computationally not possible to derive from $\boldsymbol{E_K}$.
- For each K, it is feasible to compute the inverse pairs $\boldsymbol{E_K}$ and $\boldsymbol{D_K}$ from K.

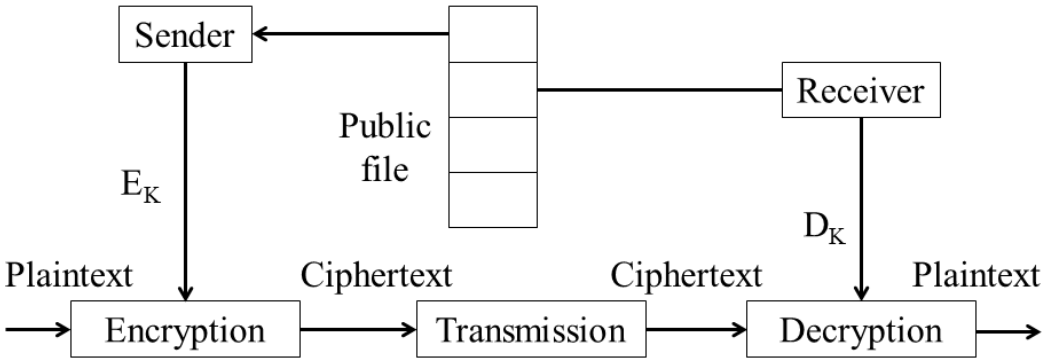


Figure 3.3: Public Key Cryptosystem

The third property of PKC makes it more secure, as the encryption key $\boldsymbol{E_K}$ of every user is made public without sacrificing the security of his private key, which is decryption key $\boldsymbol{D_K}$ [52]. The public key cryptographic system is thus divided into two parts, encryption transformations and decryption transformations, such that if one set of transformations are made available, even then it is impractical to find other set of transformations.

The forth property ensures that it is feasible to compute corresponding pairs of transformations without implementing any constraints like what the encryption or decryption transformation can be.

In public key cryptosystem, there is no need to share the secret key through a secure channel. Every user in the system has one pair of keys, one is a public encryption key $\boldsymbol{E_{KA}}$, which is made public and anyone in the system have access to this key and the other key is private decryption key $\boldsymbol{D_{KA}}$, which is available to the owner of this key only [51]. With the help of user's private key, a user can calculate his corresponding public key, but the reverse is not possible, that is even if someone has access to a user's public key, still he is unable to compute the private key from that available public key. The RSA and ElGamal cryptosystems are successful examples of public cryptosystem.

All public keys are publically available to all the users on network; they might be stored in a public file, such as in a phone book [52]. However the private keys are kept secret and are available only to the owner of that key.

3.2.1 WORKING OF PUBLIC KEY CRYPTOSYSTEM (PKC)

Consider that user A wants to send message m to user B. The entire process works as follows:

- User A looks up for the public key $\boldsymbol{E_{KB}}$ of user B, then encrypt the message m as:

$$E_{KB}(m) = C \tag{3.4}$$

  And send the cipher-text C to user B.
- Since user B has the corresponding decryption key $\boldsymbol{D_{KB}}$ therefore B is able to decrypt the message from received cipher-text.

$$D_{KB}(C) = D_{KB}(E_{KB}(m)) = m \quad (3.5)$$

- No other user can decrypt the message because it is infeasible to compute the $\boldsymbol{D_{KB}}$ from $\boldsymbol{E_{KB}}$.

3.2.2 ADVANTAGES OF PKC

Some noteworthy advantages of using public or Asymmetric key cryptography are: no secret key needs to be shared among the users, each user needs relatively few keys, and any new user can join the existing cryptosystem without disturbing the old users, separate keys are used for encryption and decryption and hence secure communication is achieved over the public channel for users who have never met. It provides nonrepudiation and example of PKC is digital signatures schemes.

3.3 PROPERTIES OF DIGITAL SIGNATURES

The various properties of digital signatures are shown in figure 3.4 and are discussed as follows:

- The signatures must be unforgeable and infeasible to be reused, which means no one except the signer can sign the document [53]. Therefore the receiving authority is convinced that the signer purposefully signed the document.
- The digital signatures ensure the authenticity of the signer.
- Finally, the above two properties (authenticity and unforgeability) ensures the non-repudiation of the signature, which means the signer cannot deny that he did not sign the document or message [53].

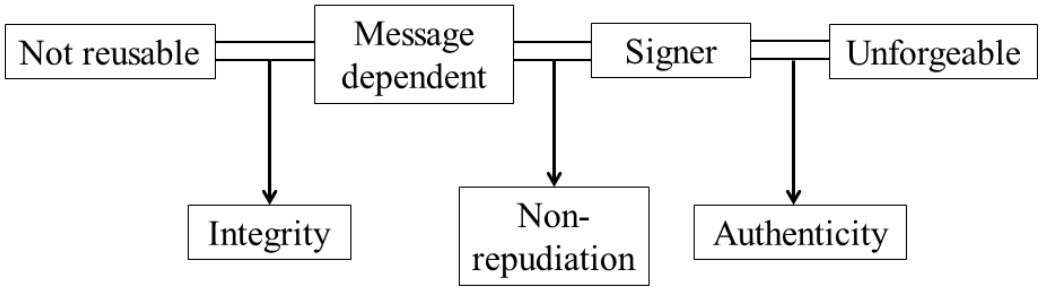


Figure 3.4: Properties of Digital Signature

3.4 SIGNATURES AND THE LEGALITIES

Signature is not a part of the transaction or message, but rather an expression or important detail of the signing authority that help in authentication process. Main purposes of signature writings are as given below:

a) **Evidence:** A signature whether its handwritten or a digital, authenticates a document by identifying the signer with the signed document. When the signer makes a mark in unique manner, the document becomes attributable to the signer.
b) **Ceremony:** The process of signing a document calls the legal significance of the signers act and thus, helps to prevent insensitive engagements.
c) **Approval:** According to certain context defined by custom and law, a signature states the signer's authorization or approval of the writing, or the signer's intention that it has legal effect.
d) **Efficiency and Logistics:** A handwritten signature on a document often conveys a sense of clarity and inevitability to the transaction and lessens the need to inquire past the face of a document.

The formal requirements for legal documentation, including the need for signatures, differ in different legal systems, and also vary over a period of time [51]. There is also modification in the legal consequences of failure to cast the transaction in an essential form. The act of frauds of common law tradition does not mark a document invalid for lack of written signatures by the authority to be charged, but rather it makes it unenforceable in court, which limits the practical application of the act in case of law.

During this century, most of the legal systems have reduced the formal requirements or minimized the chances of failure to satisfy the formal requirements. Sound practice for transactions is still formalized in a manner that assures the parties of their enforceability and validity [52]. In current practice, formalization involves documenting the transaction on paper and authenticating the paper by signing. However, traditional methods are undergoing fundamental change.

In many circumstances or due to the modern world, the information needed to exchange to effect a transaction never takes paper form, instead computer based information is utilized differently than its paper counterpart. In computers, digital information can be stored and transformed, based on the information some programmable actions can be taken. Information stored in digital format as bits rather than ink and paper can be transferred near the speed of light.

Although the basic nature of transaction remains same, the law has now started to adopt the advancement in technology [53]. Therefore, the legal and business communities need to develop rules and practices that use new technologies to achieve the effects historically expected from the paper forms.

To achieve the basic effectiveness of signatures described above, a signature must have these attributes:

a) **Signer authentication:** A signature should contain the unique information of signing authority, such that the receiving authority can know who signed that document, record or message [53]. Also it should be impracticable for another person to regenerate same signature without authority.
b) **Document authentication:** A signature should identify the document that is signed. In case of digital signature, it must be unique for different documents with same signer that means the signature should contain the information along with the document information. This property of signatures makes it practically impossible to falsify or alter the signed document or signature without detection.

   Signer and documentation authentication are effective tools used to avoid impersonators and forgers. In the information security profession terminology, it is known as a non-repudiation service. It provides assurance of data to protect the signer against false denial by recipient or protects the recipient against false denial by signing authority [53]. Hence, this service provides evidence to prevent a person from tampering or terminating legal obligations arising of a transaction effected by computer-based systems.

a) **Affirmative act:** The affixing of signature should be a confirmatory act that serves the ceremonial and approves functions of a signature and establishes a legal value of the transaction.

b) **Efficiency:** A signature and its generation and verification processes should provide the highest possible assurance of both document authenticity and signer authenticity, with the minimum possible expenditure of resources.

3.5 CLASSIFICATION OF DIGITAL SIGNATURE SCHEMES

The taxonomy of digital signatures is shown in figure 3.5. There are only two classes of digital signature schemes that are, digital signature scheme with appendix and digital signature schemes with message recovery [54]. The first one requires the original message as an input for verification process and the other one do not require original message for verification process.

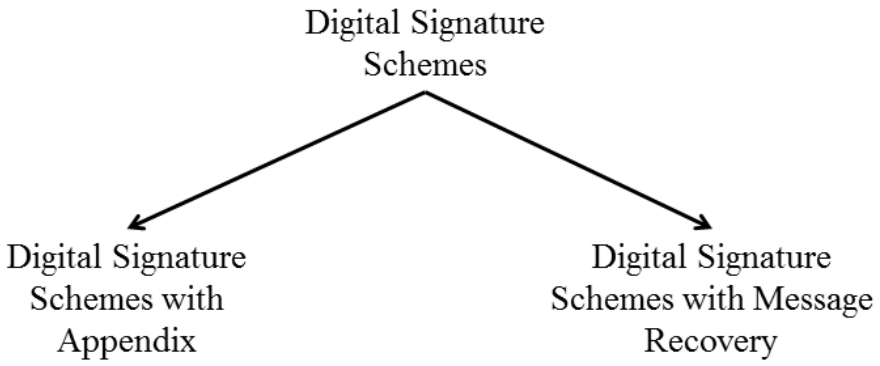


Figure 3.5: Classification of digital signature schemes

3.5.1 DIGITAL SIGNATURE SCHEMES WITH APPENDIX

Digital signature schemes with appendix depend on cryptographic hash function h. DSA, Schonerr, ElGamal signature scheme are examples of such digital signature schemes. A priori knowledge of original message is necessary for the verification algorithm [55]. In these schemes, a user A can create a signature $s \epsilon S$, (where S is a set of elements known as signature space) for a message $m \epsilon M$, *(*where M is a set of elements known as message space), which can be verified by some other user B.

Each user A selects a unique secret key S_A from the set

$$S_{A,k} : k \in R \tag{3.6}$$

where $S_{A,K}$ is a signing transformation and it is one to one mapping from M_h to S,

R is known as indexing set of signing,

M_h is the image of hash function h i.e. $h: M \to M_h$; $M_h \subseteq M_s$ (M_s is a set of elements called signing space, M_h is called hash value space),

S_A defines the mapping of V_A from $M_h \times S$ to true or false, such that

$$V_A(m_h, s) = \begin{cases} True & , if\ S_{A,k}(m_h) = s \\ False & , otherwise \end{cases} \tag{3.7}$$

for all messages $m_h \in M_h$ and $s \in S$, here,

$$m_h = h(m) \qquad \text{for } m \in M \tag{3.8}$$

V_A is the public key of signer and is also known as verification transformation and is designed in such a way that it can be computed without any knowledge of the signer's secret key S_A.

Signing process is shown in figure 3.6 and the steps to generate the signature are as follows:

- The signer selects his secret key S_A and element $k \in R$ and computes

$$m_h = h(m) \quad \text{and} \quad s = S_{A,k}(m_h) \tag{3.9}$$

  Where h is a one way hash function.

- The pair of s, m_h is the signature attached with the message m and send to the user B.

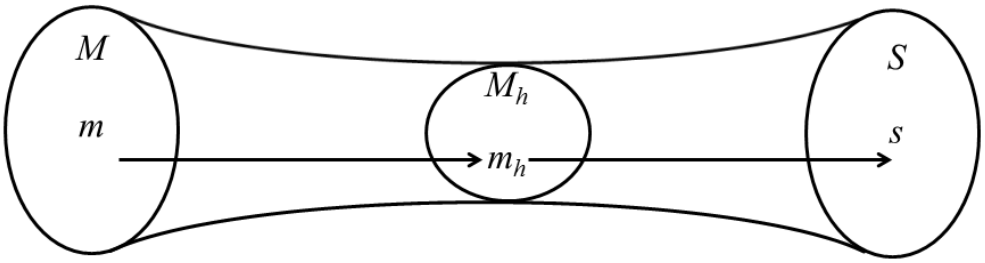


Figure 3.6: The Signing Process [55]

Signature verification process is shown in figure3.7 and the steps to verify the signature are:

- User B obtains the public key of the signing authority, in this case it is user A and computes message hash

$$m_h = h(m) \quad \text{and} \quad \text{u} = V_A(m_h, s) \tag{3.10}$$

- The user B accepts the signature only if u comes out to be TRUE.

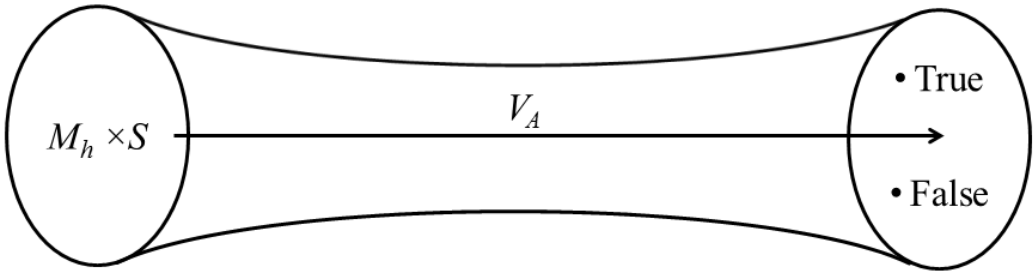


Figure 3.7: The Verification Process [55]

3.5.2 DIGITAL SIGNATURE SCHEME WITH MESSAGE RECOVERY

Digital signature with message recovery allows the user to recover the original message from the signature itself. Therefore a priori knowledge is not necessary for the verification algorithm [56]. These schemes are best useful for short messages. Examples of such digital signature schemes are: RSA, Rabin and Nyberg-Rueppel.

Signing process is shown in figure 3.8 and the steps to generate the signature are as follows:

- User A selects an element $k \in R$ and selects his secret key S_A and computes

$$m_h = \xi(m) \quad \text{and} \quad s = S_{A,k}(m_h) \tag{3.11}$$

  where ξ is one to one mapping of M to M_s.

- s is the signature attached to the message m and then send to the user B.

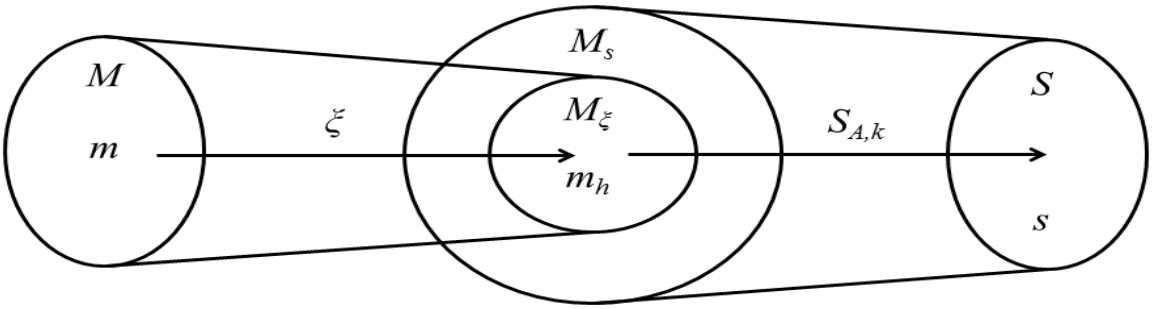


Figure 3.8: Digital Signature with Message Recovery [56]

Steps to verify the signature are:

- User B searches for the public key of sender A and computes $m_h = V_A(s)$ and verifies if $m_h \in M_\xi$ (image of ξ), or not. If m_h does not belongs to M_ξ then the signature is rejected.
- If the signature is successfully verified, then user B recovers the original message from m_h by computing $\xi^{-1}(m_h)$.

3.6 DIGITAL SIGNATURE TECHNIQUES

Digital signatures come under the branch of cryptography and are created and verified by the cryptographic tools. Cryptography concerns itself with converting the original message into unintelligent forms and back again [56]. Digital Signatures are an example of public key cryptography that employs two different keys for signing a document and verifying that signature at the receiving end. Various digital signature schemes are as follows:

3.6.1 THE RSA SIGNATURE SCHEME

RSA was named after three people who were to make the most spectacular contribution in the field of public key cryptography: Ronald Rivest, Adi Shamir and Leonard Adleman. RSA digital signature scheme was the first scheme with message recovery feature. It is one of the most versatile and practical techniques available [57]. The signing space, message space, cipher-text space and signature space for this scheme belongs to $Zn = (0,1,2,3,\ldots.\mathrm{n}-1)$, where $n = p * q$ is the multiplication of two randomly chosen prime numbers p, q

Steps for signing a message $m \in M$,

- The signing authority or user A computes $m_h = \xi(m)$.
- Applying his private key d, he computes $s = (m_h)^d \bmod n$.
- s is the signature of user A generated from the above scheme for an input message m.

Steps to verify the signature s and recover the message m,

- The receiving party or user B applies the public key e of the signer (user A) and computes

$$m_h = (s)^e \bmod n \tag{3.12}$$

- Verify that $m_h \in M_\xi$, if yes only then the signature is accepted and the signer is marked as authentic.
- User B recovers the original message by $m = \xi^{-1}(m_h)$.

3.6.2 FEIGE-FIAT-SHAMIR SIGNATURE SCHEME

This scheme falls under the category of digital signature schemes with appendix. It requires a one way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^k$ for a fixed positive integer valued k. Here $\{0,1\}^k$ represents the set of bit strings of k bit length and $\{0,1\}^*$ is a set of all bit strings of any bit length [58]. In this scheme

- Each user A selects a non-negative integer k and random integers s_j such that $s_j \in Z_n^*$, where $j = 1, 2, 3, ...k$ and $n = p.q$.
- User A computes $v_j = s_j^{-2} \bmod n$.
- The k-tuple (s_j) is the private key and the k-tuple (v_j) is the public key of user A.

Steps to generate the signature for message m

- User A selects a random number r, such that $r \in Z_n^*$ and computes $u = r^2 \bmod n$.
- User A computes $e = (e_j) = h(m//u)$, each $e_j \in \{0,1\}$.
- User A also computes $s = r.\prod_{j=1}^{k} s_j^{e_j} \bmod n$.
- Final signature of the user A for the message m is (e, s, m)

Steps to verify the signature by user B

- User B computes $w = s^2 . \prod_{j=1}^{k} v_j^{e_j} \bmod n$.
- It also computes $\overset{\vee}{e} = h(m//u)$.
- User B accepts the signature if $e = \overset{\vee}{e}$.

Unlike the RSA digital signature scheme, all users are allowed to use the same modulus $n = p * q$. A key distribution center is required to generate the public and private key pairs and the two randomly chosen prime numbers p, q for each user.

3.6.3 DIGITAL SIGNATURE ALGORITHM (DSA)

The parameters required for this algorithm are as follows:

- $p = a$ is a prime modulus of L bits long where range of L is $512 \le L \le 1024$ and L is a multiple of 64.
- $q = a$ is 160 bits prime divisor of $p - 1$.
- $g = \alpha^{(p-1)/q} \bmod p$ where $\alpha \in Z_p^*$ and g is element of order q in Z_p^*.
- x_A is an integer with $0 < x_A < q$.
- $y_A = g^{x_A} \bmod p$.
- h is a one way hash function.

The parameters p, q, h and g are known as system parameters and are publically available for all the users [55]. User's public and private keys are y_A and x_A respectively. To generate a digital signature for a message of arbitrary length, the user A,

- selects a random number k and computes $k^{-1} \bmod n$.
- computes $r = (g^k \bmod p) \bmod q$.
- computes $s = k^{-1}\{h(m) + x_A . r\} \bmod q$.

The pair of r, s is the signature of user A for message m. For each new signature, a new value of k is required.

To verification the signature, the user B,

- verifies that $1 \le s \le p-1$ and $1 \le r \le p-1$, if yes, then go to next step otherwise reject the signature at this step.
- computes $w = s^{-1} \bmod p$ and $h(m)$.
- computes $u_1 = w.h(m) \bmod q$ and $u_2 = r.w \bmod q$.
- Computes $v = g^{u_1} y_A^{u2} \bmod q$.
- if $v = r$, then immediately accepts the signature.
- The security of the DSA algorithm relies on two distinct but interrelated discrete logarithm problems [55]. First one is the logarithm problem of Z_p^* and the second is the logarithm problem of cyclic subgroup of order q.

3.7 DIGITAL SIGNATURE WITH ADDITIONAL FUNCTIONALITY

There are some circumstances under which authentication are not the only requirement; some other functionality and other properties of digital signatures might be required [60]. Therefore the basic digital signature scheme is combined with a specific protocol (like The RSA, The ElGamal) to achieve the additional features that cannot be provided by the basic methods only.

Some well-known signature schemes with additional features are described below:

3.7.1 MULTI-SIGNATURE SCHEME

In many commercial or government applications, signatures of more than one authorization are required on a document. Then multi-signature schemes came into existence, as multiple keys are required for the signing process [61, 62, 63]. These signatures are useful when a new law or bill needs to pass by the mutual agreement of multiple government authorities. Multi-signatures are also useful in cases of contracts, which are required to be signed by their business partners.

3.7.2 GROUP SIGNATURE SCHEME

Let's consider a group of people, in which each member is authorized to sign the documents on the behalf of their group [64, 65, 66]. This type of signature is known as group signature. The salient features of the group signature scheme are as follows:

- Only the members of the group are allowed to sign the message.
- The receiver can check whether the signature is a valid group signature or not.
- The identity of the group member, who signed the message, does not get revealed to the receiving party.
- In case of any disputes, either the group members or a trusted third party can identify the signer.

3.7.3 UNDENIABLE SIGNATURE SCHEME

Unlike the handwritten signatures or banknote printing, the digital signatures are easy to copy exactly. It can be advantageous in some cases such as dissemination of announcements and public keys, where more copies are distributed [67, 68]. But it can be unsuitable for many other applications, such as electronic replacement for all written or oral commitments that might be personally or commercially sensitive. In these cases, the proliferation of the certified copies might facilitate improper uses like industrial espionage or blackmail. The recipient of such a case should be able to ensure that the signing authority cannot later disavow it. Also, the recipient should be forbidden or unable to show the commitment to anyone without the approval from signer.

Undeniable signatures are best suitable for the above mentioned situation [69]. An undeniable signature, like the digital signatures, is a number issued by the signer that depends on the message to be signed. Unlike the digital signatures, an undeniable signature cannot be verified without the help of signing authority.

CHAPTER 4

PROPOSED METHODOLOGY

After discussing the various schemes presented in literature, one can analyse that there is a need to design a new approach that can accurately authenticate the sender while supporting the desired modifications of image processing tools. Such an approach is discussed below that uses the concept of digital signatures to validate the sender on the basis of their secret key used. In addition, the robustness of this scheme against noisy channels makes it suitable for wireless authentication systems and other real-time applications, also the scheme can withstand with lossy compression techniques, and therefore a predefined threshold value is used to achieve the desired quality. The proposed signature scheme can be extended to more advanced form, thereby allowing users to authenticate the signer prior to the image processing, hence time could be saved in case the signer authentication fails.

4.1 PROPOSED APPROACH

To have a clear understanding of the proposed approach, the block diagram is shown in figure 4.1. It provides the layout of the designed methodology. Working of each block is discussed below in detail.

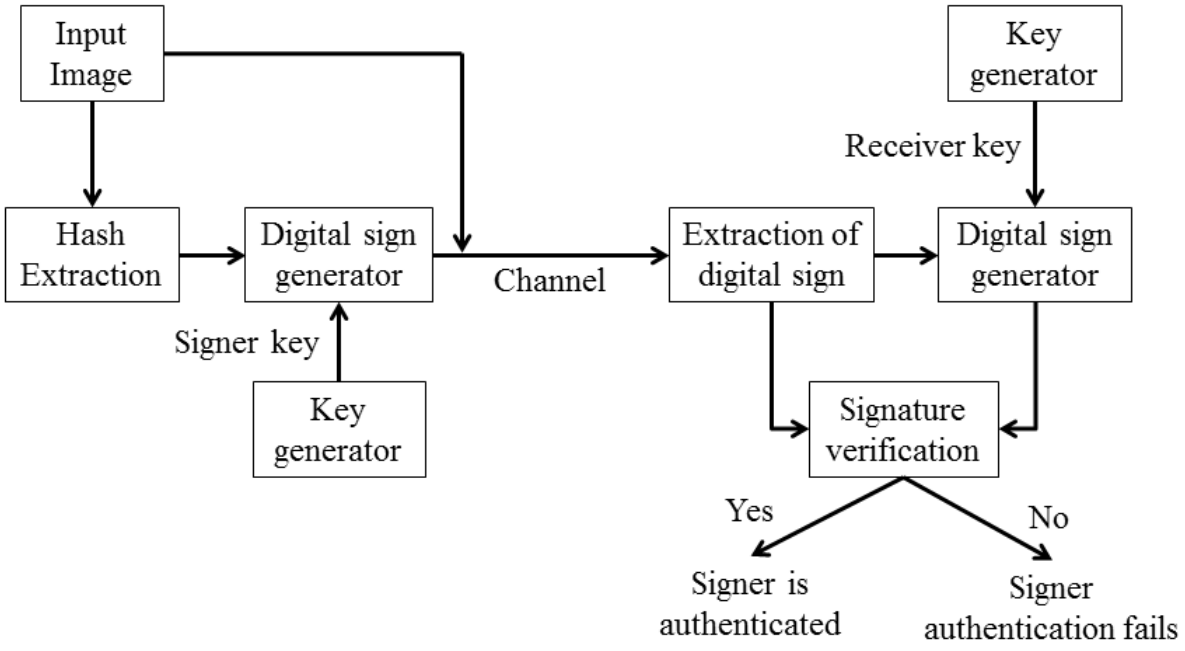


Figure 4.1: Block diagram of proposed approach

The flow chart of the proposed approach is shown in figure 4.2.

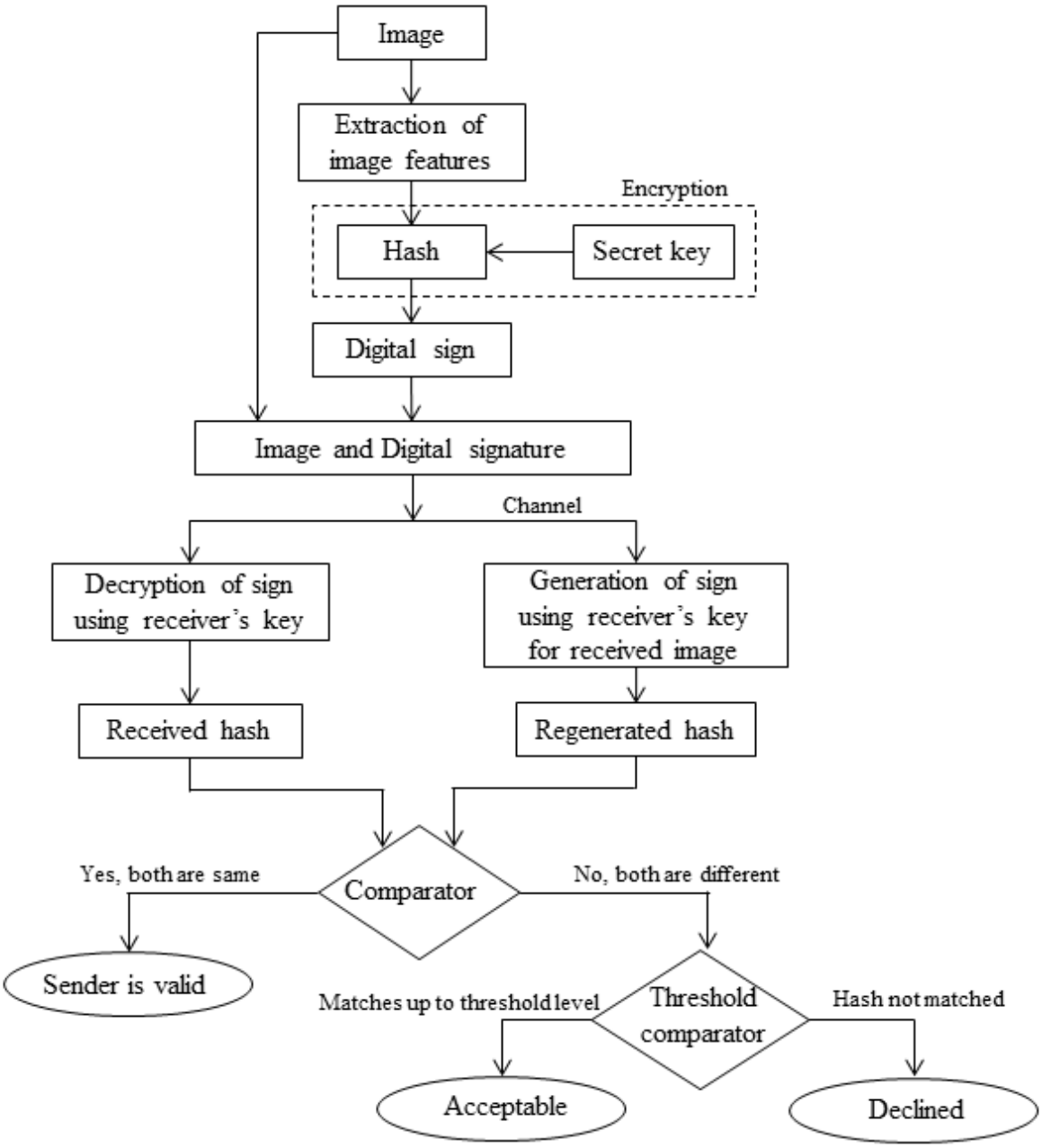


Figure 4.2: Flow chart of proposed approach

4.1.1: AT TRANSMITTING END:

a) Input Image: It is the actual digital image data that needs to be processed to generate a digital signature. This image can be of grayscale or RGB Coloured. If the image is RGB coloured then it needs that each of the colour plane i.e. Red, Green and Blue, must be processed individually and then recombined back to obtain the final signature.

i. **Zero Padding:** As per the algorithm requirements, input image should be square in dimension for the hash computations. In case the input image is not a square, then some extra zeros must be padded to make it square dimensional before the hash extraction. For example, input image is of dimension 600×600 pixels, then there is no need to of zero padding. Let the dimensions of the image be 240×256 pixels, here number of columns is greater than the number of rows, therefore some extra rows of zero will be padded to the image to make the dimensions 256×256 pixels.

b) Hash Extraction: Hash is obtained by extracting some of the features of the input image such that, if the input image is replaced with some other image, then same signature cannot not be used even if the signer remains same. Therefore it prevents forgery of the signature.

i. **Block Division:** Once the image dimensions are properly matched, then image is subdivided into M, N blocks in both row and column wise respectively. The relation between image size and block dimension can be described by eq. (4.1)

$$k = \frac{m}{M} \tag{4.1}$$

where $k \times k$ is the size of each block,

m is the number of rows of image matrix and

$M = N$ is the total number of blocks in row and column wise, selected by the mutual agreement of the sender-receiver pair. Block division is shown in figure 4.3.

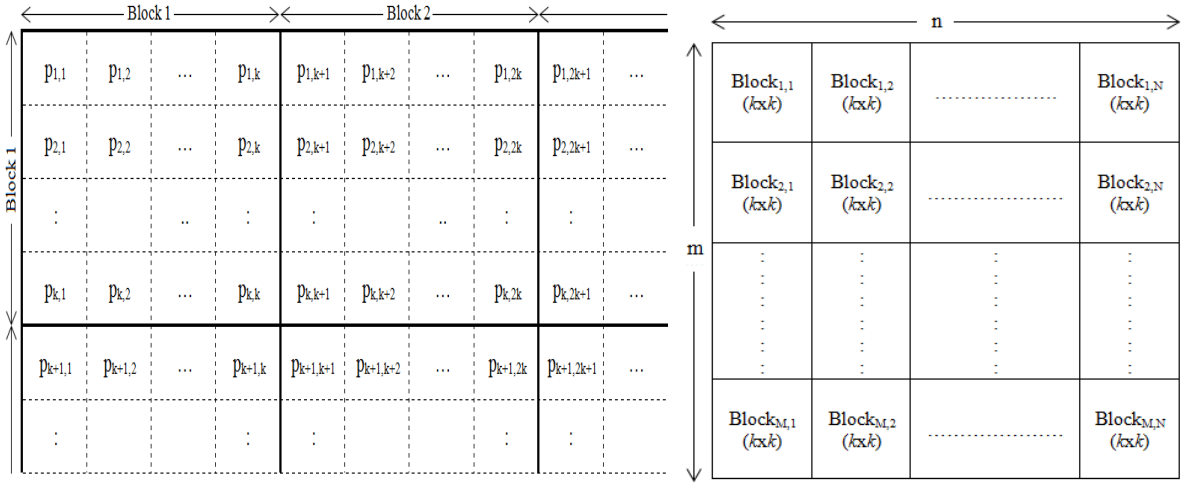


Figure 4.3: Block division of input image

M, N are responsible for the hash size and digital signature size, the hash length is $1 \times M$. Let's say the desired hash length is of 32 bytes, i.e. $M = N = 32$, $k = 8$ and each block will consist of 8×8 pixels. In case the user wants to change the length of the hash, he can vary this by increasing or decreasing the number of blocks in which input image is divided. So, the hash length is directly proportional to the number of blocks. However, if number of blocks is reduced, so as to reduce the length of the hash, the details become less significant as mean is taken of a larger block size and ultimately it affects the precision of the hash.

ii. **Generation of Mean Matrix:** Mean of all the individual blocks is calculated to generate a mean matrix of size $M \times N$. For each particular block there is a corresponding mean value in the mean matrix. Therefore it appears as the thumbnail of the input image. Formula to generate a mean matrix is given in eq. (4.2) and a block mean map of input image 'Lena' is shown in figure 4.4.

$$\mu_b\left(\text{mean}\right) = \frac{\sum_{i=1}^{k}\sum_{j=1}^{k} p_{i,j}}{k \times k} \quad ; (1,1) \le b \le (M,N) \tag{4.2}$$

where b denotes the specific block number and $p_{i,j}$ is the pixel value in image matrix for i^{th} row and j^{th} column.

Figure 4.4: Mean matrix of size 64×64 pixels

iii. Computation of Hash:

Two hash matrices are computed by performing the modulo-2 addition of each row and each column of the mean matrix. The process of hash generation is shown in figure 4.5.

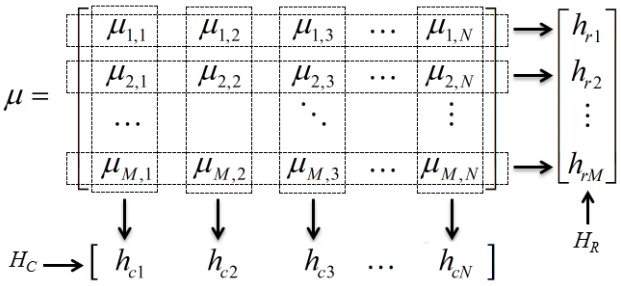


Figure 4.5: Hash matrixes generation

The hash consisting of modulo-2 addition of rows of mean matrix is termed as row hash and is defined by eq. (4.3)

$$H_R = [h_{r1} \quad h_{r2} \quad h_{r3} \quad .... \quad h_{rM}] \tag{4.3}$$

Similarly the column hash is given by eq. (4.4)

$$H_C = [h_{c1} \quad h_{c2} \quad h_{c3} \quad .... \quad h_{cN}] \tag{4.4}$$

Row and column hash matrices of lena are given in eq. (4.5)

$$H_R = [44 \quad 36 \quad 50 \quad 204 \quad 110 \quad ... \quad 26 \quad 160] \tag{4.5a}$$

$$H_C = [79 \quad 201 \quad 61 \quad 52 \quad 75 \quad ... \quad 78 \quad 203] \tag{4.5b}$$

Once the two hash matrices are obtained, final hash can be computed by using eq. (4.6).

$$H_F = H_R \oplus H_C \tag{4.6}$$

Final hash of "lena" image is given in eq. (4.7)

$$H_F = [44 \oplus 79 \quad 36 \oplus 201 \quad 50 \oplus 61 \quad 204 \oplus 61 \quad ... \quad 160 \oplus 203] \tag{4.7a}$$

$$H_F = [99 \quad 237 \quad 15 \quad 248 \quad ... \quad 107] \tag{4.7b}$$

c) Key generator: In the proposed approach, a variable length secret key is required. Key used at transmitter side is known as "signer key" and is used to sign the message whereas the key used at receiving side is known as "receiver key" and is used to verify the signatures attached with the message.

d) Digital Signature generator: It takes two inputs, one is extracted hash from the image and other is the signer key. Encryption is necessary in order to provide additional security to the hash obtained. It is the final step in the generation process of digital signature. The final hash is encrypted here by DES technique to increase its security from unknown attacks

during its transmission. It uses the same key for its encryption and decryption. If an unauthorized user gets the encrypted form of data while it is on transmission channel even then he cannot extract the original information without the knowledge of secret key used. The benefit of encrypting the hash is that only certain users who are authorised can verify the image's integrity while un-authorised users are prevented to do so.

The sender will be validated on the basis of the key used; hence it must be kept secret among the dedicated users only. Any change in the key will result a large variation in the signature generated and will be denied at receiver if same key is not used for its decryption. Digital signature obtained after encrypting the final hash of "lena" image is given in eq. (4.8).

$$L0H/GMZosuEwuG+pACqu6UZ2oYW+6vmOpL1bOdZrDl/AK/XsL3xmb/Ioyn0oOF4bvkvzOTxQOolC6D3lYnzXnuXVgy7lWuiaaVEbVe+C1fRO7j7+W S5Ig/zluJdIStcEmb3jNNYaFj0xQQJdYRcN5g== \quad (4.8)$$

After the digital signature is obtained, it is transmitted along with the input image to the recipient through the wired or wireless channel. The transmitted data is shown in the figure 4.6.

+ Digital Signature

Figure 4.6: Transmitted data

4.1.2: AT RECEIVING END:

e) Extraction of digital signature: It is the first step at the receiver. The receiver will extract the digital signature from the received data and send it to the signature verification device and the received image is forwarded to the digital sign generator.

f) Digital sign Generator: This is same as the one used at the transmission side. It takes the receiver key which is kept same as the signer key, and processes the received image to

produce its digital signature. This digital signature is then forwarded to the signature verification unit, where it is compared to validate the signer.

However, noise may get introduced in the image during its transmission, or the compressed image might be transferred to save the bandwidth, but it might be possible that the received image could not be properly decompressed; therefore the digital signature generated at the receiving end can differ from the original signatures. Hence a threshold level is mutually decided by the signer and receiver. If both the signatures shows similarity up to the threshold level, only then signer will be marked at as authentic user.

g) Signature verification: Both the digital signatures are fed to signature verification unit. Any mismatch between these two can be a result of corrupt pixel or a tampered image. A threshold level can be set to support the lossy compression techniques, up to which the image will be marked as acceptable otherwise the retransmission of image will be required.

4.2 ADVANCED PROPOSED APPROACH

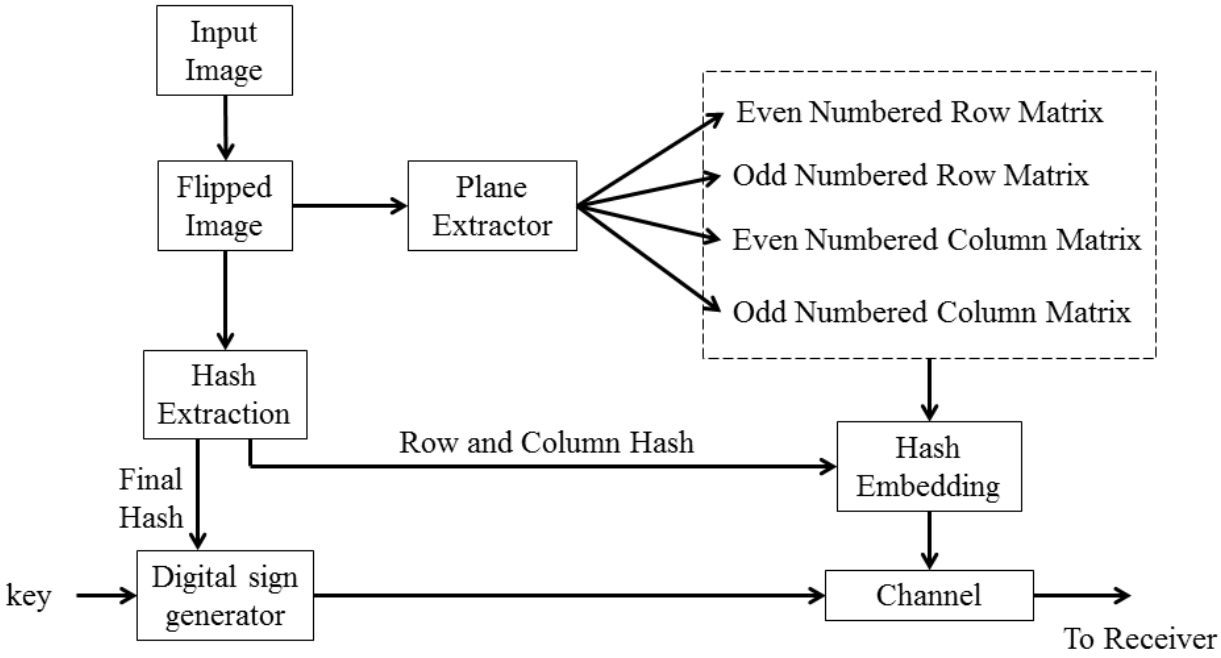


Figure 4.7: Block diagram of advanced transmitter

In the above mentioned scheme, the input image is sent without any changes and a digital signature is sent along with it, but if the image is sent with some manipulations such that no other can read it without the knowledge of the scheme, this can help in improving the confidentiality and data integrity. Such advancement is done on the above mentioned scheme and the new digital signature scheme is described below. The block diagram of advanced proposed signature scheme is shown in figure 4.7.

4.2.1 AT TRANSMITTING END:

a) Input Image: It is the actual digital image data that needs to be processed to generate a digital signature. This image can be of grayscale or RGB Coloured. If the image is RGB coloured then it needs that each of the colour plane i.e. Red, Green and Blue, must be processed individually and then recombined back to obtain the final signature. The image dimensions required for this proposed approach should be $M \times M$ i.e. number of rows and columns should be equal, if not, zero padding could be done to make the dimensions equal.

b) Flipped Image: All the pixel values from the input image are flipped in this step, to make the image appears more random to an unknown user. The process of flipping the pixel values is shown in figure 4.8

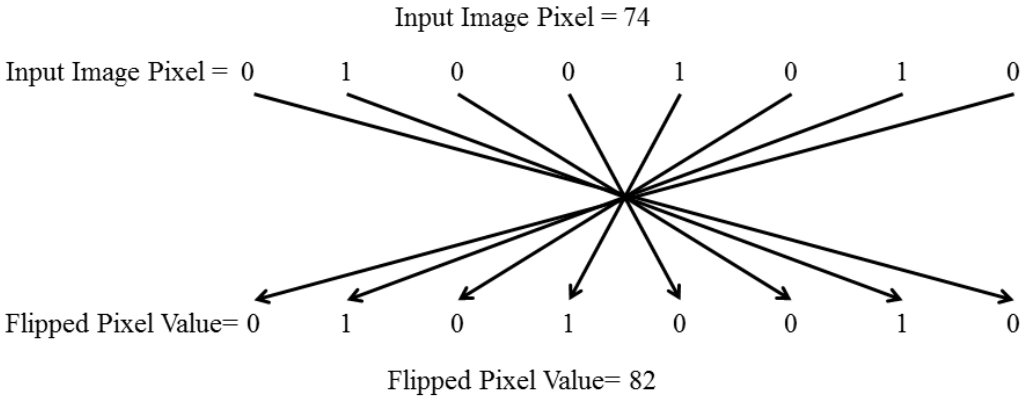


Figure 4.8: Process of flipping pixel values

c) Plane Extractor: Four planes of the input image after flipping are extracted such that, first plane consists only the even numbered row pixels of the flipped input image and is termed as Even Numbered Row Matrix, second plane consists of odd numbered rows pixels and is

known as Odd Numbered Row Matrix. Similarly Even Numbered Column Matrix and Odd Numbered Column Matrix are also extracted from the input image. The flipped input image matrix is given in eq. (4.9)

$$I = \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & \cdots & p_{1,N} \\ p_{2,1} & p_{2,2} & p_{2,3} & \cdots & p_{2,N} \\ \cdots & & \ddots & & \vdots \\ p_{M,1} & p_{M,2} & p_{M,3} & \cdots & p_{M,N} \end{bmatrix}_{M \times N} \tag{4.9}$$

where I is the input image of size $M \times N$ and

$p_{i,j}$ denotes the pixel in i^{th} row and j^{th} column of input image matrix.

Four planes that are extracted from the input image are shown in eq. (4.10a) and eq. (4.10b), where E_R denotes the Even Numbered Row Matrix, O_R is the Odd Numbered Row Matrix and E_C, O_C represents the Even and Odd Column Matrices respectively.

$$E_R = \begin{bmatrix} p_{2,1} & p_{2,2} & \cdots & p_{2,N} \\ p_{4,1} & p_{4,2} & \cdots & p_{4,N} \\ \cdots & & \ddots & \vdots \\ p_{M,1} & p_{M,2} & \cdots & p_{M,N} \end{bmatrix} \text{ and } O_R = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,N} \\ p_{3,1} & p_{3,2} & \cdots & p_{3,N} \\ \cdots & & \ddots & \vdots \\ p_{M-1,1} & & \cdots & p_{M-1,N} \end{bmatrix} \tag{4.10a}$$

$$E_C = \begin{bmatrix} p_{1,2} & p_{1,4} & \cdots & p_{1,N} \\ p_{2,2} & p_{2,4} & \cdots & p_{2,N} \\ \cdots & & \ddots & \vdots \\ p_{M,2} & p_{M,4} & \cdots & p_{M,N} \end{bmatrix} \text{ and } O_C = \begin{bmatrix} p_{1,1} & p_{1,3} & \cdots & p_{1,N-1} \\ p_{2,1} & p_{2,3} & \cdots & p_{2,N-1} \\ \cdots & & & \vdots \\ p_{M,1} & p_{M,3} & \cdots & p_{M,N-1} \end{bmatrix} \tag{4.10b}$$

Size of E_R, O_R in eq. (4.10a) is $\frac{M}{2} \times N$, whereas dimension of E_C, O_C in eq. (4.10b) is $M \times \frac{N}{2}$.

d) Hash Extraction: Hash extraction process remains same as it was described in section 4.1.1. The input image is divided into M, N number of blocks in both rows and columns wise respectively. And then a mean map of above said is drawn for the computation of Row and Column hash matrices. Both these hash matrices are XORed together to make the final hash.

e) Hash Embedding: The dimensions of even and odd numbered row matrices is same, therefore at the receiving end it can become difficult to judge which matrix resembles the even or odd numbered row matrix of the input image. Hence an extra row consisting of row hash data is embedded as the last row of even numbered row matrix, and now receiver knows that even numbered row matrix will have exactly one extra row than the odd numbered row matrix, which helps in identifying both these matrices. Similarly column hash data is embedded as last column of the even numbered column matrix. The new matrices after hash embedding are given in eq. (4.11)

$$E_{R-new} = \begin{bmatrix} p_{2,1} & p_{2,2} & \cdots & p_{2,N} \\ \vdots & & \ddots & \vdots \\ p_{M,1} & & \cdots & p_{M,N} \\ C_{c1} & C_{c2} & \cdots & C_{cN} \end{bmatrix}_{\left(\frac{M}{2}+1\right)\times N} \quad \text{and} \quad E_{C-new} = \begin{bmatrix} p_{1,2} & p_{1,4} & \cdots & p_{1,N} & C_{r1} \\ p_{2,2} & p_{2,4} & \cdots & p_{2,N} & C_{r2} \\ \vdots & & & \vdots & \vdots \\ p_{M,2} & p_{M,4} & \cdots & p_{M,N} & C_{rM} \end{bmatrix}_{M\times\left(\frac{N}{2}+1\right)} \tag{4.11}$$

f) Digital sign generator: The final hash obtained from the hash extractor is then encrypted by applying the signer key to generate the digital signature, which is then ready to send to the receiving authority along with the four planes of input image.

4.2.2 AT RECEIVING END:

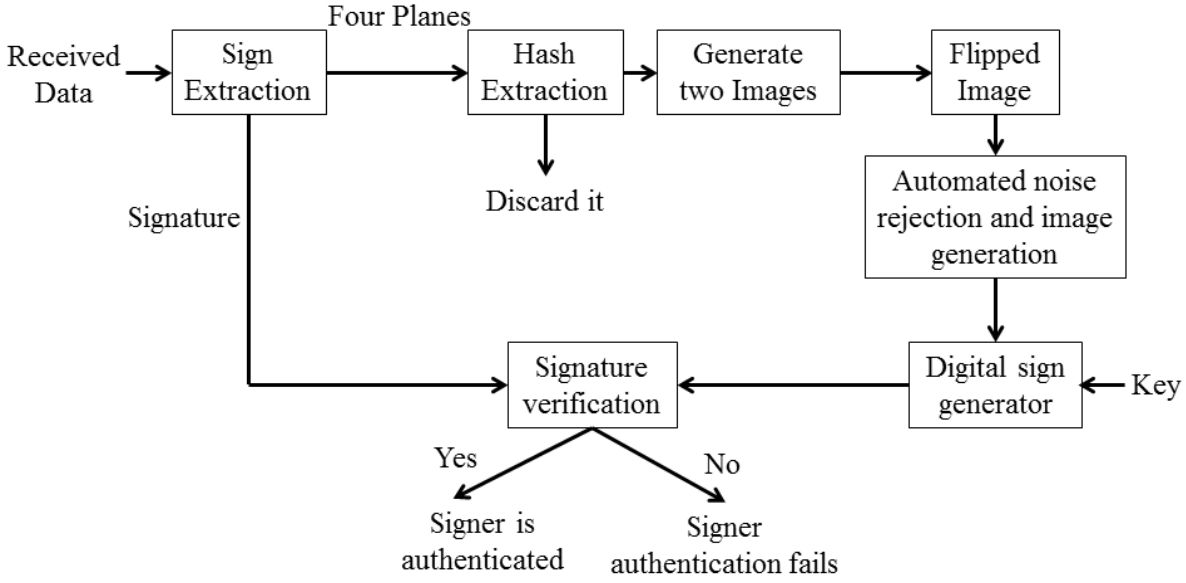


Figure 4.9: Block diagram of receiver of advanced proposed methodology

g) Sign Extraction: Once the transmitted data is finally received at receiver. The first step is to extract the digital signature from the received data and send the remaining four planes to hash extractor. The basic block diagram of the receiver is shown in figure 4.9.

h) Hash Extraction: Even numbered row matrix and Even numbered column matrix are identified by the extra row or column that was embedded into these matrices to change their dimension from the odd numbered row and column matrices. After their detection, the extra row and column hash is extracted from these matrices and all the four planes or matrices further sent to automated noise removal.

i) Generate two images: The main purpose of sending four planes of the input image is to generate two copies of the image at the receiver by using these planes. As we know noise is random in nature, so the impact of noise will not be same for all the planes and hence two images so formed from these planes will have different noise levels. The first image will formed by using the even numbered row matrix and odd numbered row matrix, second image will be generated by combining the even numbered column matrix and odd numbered column matrix.

j) Flip image: It is the inverse process of the transmitter to obtain the original pixel values from their flipped versions. All the pixel values from both the images are flipped to obtain the actual image values. And then these images are send to further compare and noise removal process.

k) Automatic noise removal and Final image generation: A comparison algorithm is designed such that it will compare the pixel values from the two images. If both values comes out to be same, then it will be directly updated in the final image, otherwise a 3×3 window will be selected across that pixel in both images. Here, normalized Euclidean distance is calculated for both windows and the window offering lesser value of Euclidean distance is selected and the faulty pixel is then replaced by the mean or average value of that window and finally that new value is updated in the final image. Normalized Euclidean distance (d) for a 3×3 window is given in eq. (4.12)

$$d(x,\alpha_i)=\sqrt{\sum_i \frac{(x-\alpha_i)^2}{\sigma^2}} \quad ;1\le i\le 9 \tag{4.12}$$

where x is the corrupt pixel value,

$\alpha_i$represents the actual pixel value of selected 3 × 3 window and

σ denotes standard deviation and is given by eq.(4.13)

$$\sigma=\sqrt{\text{var}} \tag{4.13}$$

$$\text{var}(\text{var}\,iance)=\frac{1}{K}\sum_{i=1}^{K}\left(a_i-E(\alpha)\right)^2 \quad ; K=3\times 3=9 \tag{4.14}$$

where α varies from [1,1] to [3,3]i.e all pixels of the selected window and

$E(\alpha)$ is the mean of the 3 × 3 window.

Same process is repeated until all the pixels get processed and the final image is generated.

l) Digital Sign Generator: The digital sign of the final image is generated by the same process of hash generation of image and then by encrypting the hash by receiver key. Furthermore, this digital signature generated for the received image is then send for the verification of signer by comparing it with the received signatures.

m) Signature Verification: The received signature is compared with the signature generated at the receiver side, if both the signatures show similarity upto some predefined threshold level, only then the signing authority will be marked as authentic otherwise the received data will be considered as tampered.

4.3 ADVANTAGES OF ADVANCED PROPOSED APPROACH

The main enhancements that are included in the advanced scheme are as follows

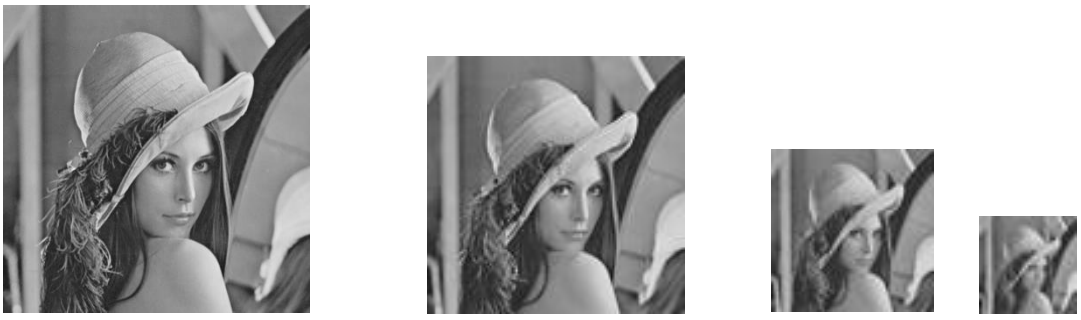
- No need to encrypt an image for secure transmission, as this approach sends the flipped version of original image by dividing it into four planes that are completely unintelligible for an unknown user without the knowledge of the combining technique used.
- Less time consuming and yet more secure as compare to the previously proposed scheme in section 4.1.

- More secure as original image is not directly transmitted through the channel.
- Automatic noise removal is another beneficial key feature of the advanced scheme, as we all know no channel is completely noise free, therefore the inbuilt noise removal algorithm helps in better quality output at the receiving end.
- High precision can be achieved while comparing the received digital signature with the digital signature generated for the new image that is the result of noise removal algorithm.
- Errors have been minimised, which results in decreasing the FRR (False Rejection Ratio) and FAR (False Acceptance Ratio) ratios.

CHAPTER 5

RESULTS AND DISCUSSIONS

By working on the proposed approach, following results have been computed. Starting with the variable hash length case, in which the input image is kept same.



(a) (b) (c) (d)

Figure 5.1: Application of proposed approach on 'Lena' Image

Figure 5.1 (a) shows the original image required to be transmitted safely (b) mean map of input image with hash length 1×64 bytes (c) mean map of input image with hash length 1×32 bytes (d) mean map of input image with hash length 1×16 bytes.

5.1 PERFORMANCE ANALYSIS OF PROPOSED APPROACH

This section shows the performance details of the proposed approach discussed in chapter4.

5.1.1 BANDWIDTH UTILIZATION

The digital signature of mean map image shown in figure 5.1 (b) is given below:

/NiK+yUmCy0CoDTHr6c//wd8NgPoMU38pzs6XDh0cIqMiIUnHcJS3cjs4m/EBhXEmtr7mCqO5dfJki8klJMTrIB2T5uMXRrYGUPVagddn/VkrYGf1S0wdnRNFBEV5y8OmilZlkfPbQds2uKbJMHf6YPyU6Vad0Eg2YWjZpIZWP4/xODkchzmVy+LFkXD6cYO/2Lyzr8jVuKXxvdMfEY/Fu7XibYDseXrzDpvfmBwg5Of4gdMTYYWdadHcqjDYuIqQgWqZa9q+eF7dRvegdmumaPme1kTI4GKUZueM/qT6WQ=

Number of bits required to transfer above digital signature is calculated in eq. (5.1)

$$Bit\ Count = 300 \times 4 = 1200\ bits \tag{5.1}$$

The digital signature for mean map image shown in figure 5.1 (c) is given below:

IcueRyD+CaVacZ+U1HmATgT7/aSnRx5nMh2p6gqXwm/SnAKtIT+ZX6IAnVB4C3aPGO UXfJaEBrqJx3Nz3PStqLzkc31uZK3k6v3yD8Ig/4lYeVHWr3Xpu6TUuIEIH9UEuSCG+r2oj VGhscUZ7lalQBu4uQLzOV9I

Number of bits required to transfer above digital signature is calculated in eq. (5.2)

$$Bit\ Count = 160 \times 4 = 640\ bits \tag{5.2}$$

The digital signature of mean map image shown in figure 5.1 (d) is given below:

C0qta8WFqJYp/rAy24jA7HZV8Lz4cvJWblQNIqvxJJCF66RlIz4HtE+KRkBeL1oPjBZUJU1 SUZlD62jNpotm6g==

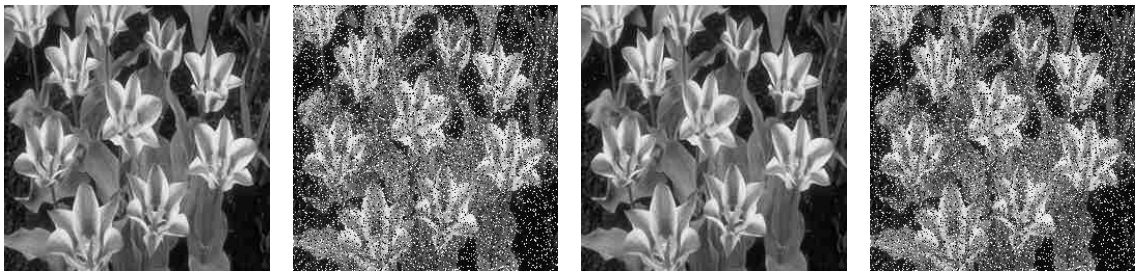
Number of bits required to transfer above digital signature is calculated in eq. (5.3)

$$Bit\ Count = 88 \times 4 = 352\ bits \tag{5.3}$$

One can easily analyse how the length of signature will affect the limited bandwidth. Larger the signature length, more bandwidth it will utilize.

5.1.2 LOSSY COMPRESSION

The proposed scheme also supports the lossy compression techniques and prevents the false rejection of signing authority. Example of compressed and uncompressed case is shown in figure 5.2.



(a) (b) (c) (d)

Figure 5.2: Application of proposed approach on 'Tullip' Image

Figure 5.2 (a) Transmitted uncompressed image (b) Received image (corrupted by noise only) (c) Transmitted compressed image (d) Received image (compressed and noise corrupted)

Root Mean Square Error (RMSE): The comparison between decrypted and regenerated hash is done on the basis of RMSE value. It is used to generate the difference between predicted values and the observed values by using an estimator. It is a good measure of accuracy and defines how much quality is preserved in the observed data. Let Hdec be the hash obtained by decrypting the digital signature and Hregen be the hash of received image. Let's say if 80% of the original image data is preserved in the received image then it will be marked as accepted and sender will be marked as authentic i.e. the RMSE of observed hash must be less than 125. RMSE can be computed by using eq. (5.4)

$$RMSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(O_{i,j} - R_{i,j}\right)^2}{M \times N}} \tag{5.4}$$

where $O_{i,j}$denotes pixel value of original image (without noise),

$R_{i,j}$denotes pixel values of recovered image and

M and N are number of rows and columns of image.

Digital signature of figure 5.2 (a) is

MZ9xPXb4ajhkvBcodX5RvlceQMciuTz1aAqdmA1/Dmi4IHLYfFxxwPB04aF1RaUNCDgg q2zThJNwTIWnhvAWy1rbi779fYiJtox5kdwx2sESXObJn+Am7O4tRA1259PsVfe5+Aogg ZSxtunWdU1f3iz31mmCCIj4

Hash of figure 5.2(a) is shown in eq. (5.5a)

$$H_{dec} = [124 \quad 24 \quad 69 \quad 24 \quad \ldots \quad \ldots \quad 106]_{1\times 32} \tag{5.5a}$$

Whereas the hash generated for figure 5.2 (b) is shown in eq. (5.5b)

$$H_{regen} = [221 \quad 214 \quad 208 \quad 195 \quad \ldots \quad \ldots \quad 211]_{1\times 32} \tag{5.5b}$$

As no channel is an ideal one in all practical applications; therefore, noise always interfere with the image data during its transmission, hence the regenerated hash will differ from the decrypted hash. The comparator will compare both these hash strings, in order to check if the noise level is acceptable or not. The RMSE comes out to be 102.4 which is less than the threshold level of RMSE=125, which means the amount to noise present in the received image is acceptable to mark the sender as authentic user.

Digital signature of figure 5.2 (c) is

J5cjMoPOIM5Sbr6KeV5WGFCyFAxx6DWMRhpoL+wH+oGtJSHzDkbNAPVXlgNWRphX58W+yar9SZqROWngnHziJ/eD7fK/Eg93C65ZoNJapmgD8V46FKa57kHwb3Q3G4ybCfk0m+fpzjgVUZsbLXwe79Ds40tHDxkM

Hash of figure 5.2(c) is shown in eq. (5.6)

$$H_{Dec} = [115 \quad 117 \quad 70 \quad 19 \quad \ldots \quad \ldots \quad 123]_{1\times 32} \tag{5.6}$$

Whereas the hash generated for figure 5.2 (d) is shown in eq. (5.7)

$$H_{regen} = [149 \quad 105 \quad 233 \quad 182 \quad \ldots \quad \ldots \quad 68\ ]_{1\times 32} \tag{5.7}$$

Comparison of both hashes resulted in mismatch, therefore next step is to check if the amount of mismatch is bearable or not, by comparing it with the threshold level of RMSE. The observed RMSE of regenerated hash from the decrypted hash comes out to be 107.89 which is less then threshold level of 125 that means even though the image is not properly decompressed at receiver but it is still acceptable and can be used for further processing.

5.1.3 TIME CONSUMPTION

Time taken for the complete signing process can be obtained by recording the whole signature generation process of the algorithm. Lesser the time taken to sign an image, faster the signing algorithm will be.

Table 5.1: Time analyses for different images of different sizes with hash length *M=32*

Image Name	Image Size (in pixel)	Block Size (in pixel)	Signature Generation Time (in sec)
Cameraman	128x128	4x4	0.0845
Barbara	256x256	8x8	0.0921
Lena	512x512	16x16	0.1001
Baboon	576x576	18x18	0.1251
Model	640x640	20x20	0.1572
Gamer	960x960	30x30	0.1759
Boat	1024x1024	32x32	0.1821

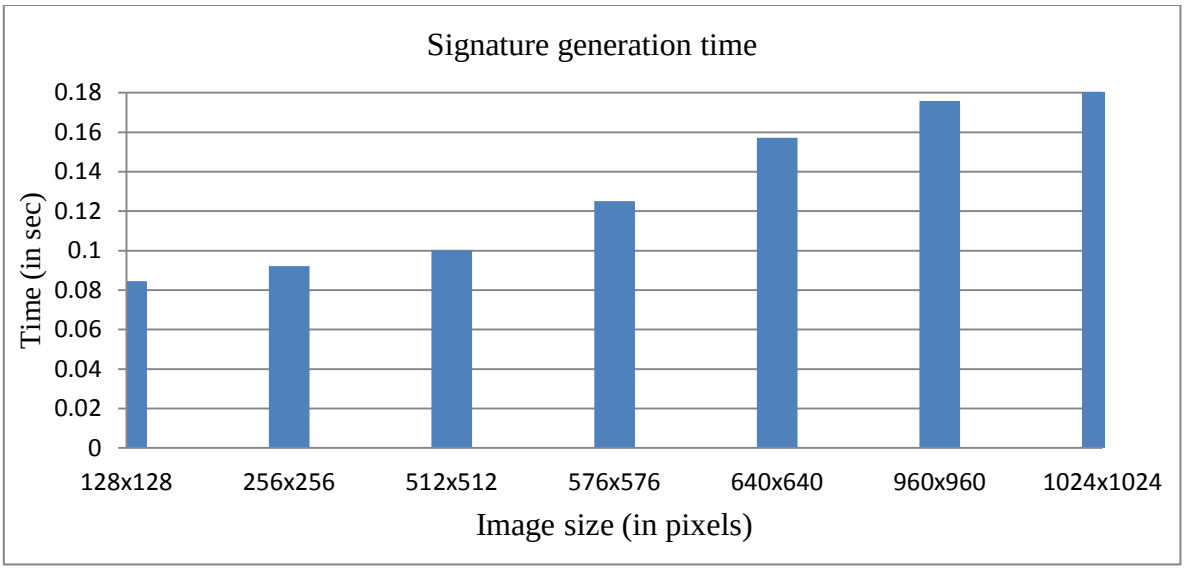


Figure 5.3: Image size vs. Generation time

From the computational analyses of Table 5.1, it has been observed that as the image size increases the signature generation time also increases exponentially. Image size vs. signature generation time plot is shown in figure 5.3.

Figure 5.4: Lenna image of size 256x256 pixels

Table 5.2: Processing time analyses for different number of block divisions for figure 5.4

Block size	Total Number of Blocks	Hash Length (in pixel)	Signature Generation Time (sec)
4x4	16384	1x128	3.216
8x8	4096	1x64	1.1277
16x16	1024	1x32	0.2693
32x32	256	1x16	0.1249
64x64	64	1x8	0.0628

Table 5.2 shows the impact of variable hash length on the signature generation time. For better analysis, the image size is kept same for all different hash lengths. Block size vs. signature generation time plot is shown in figure 5.5.

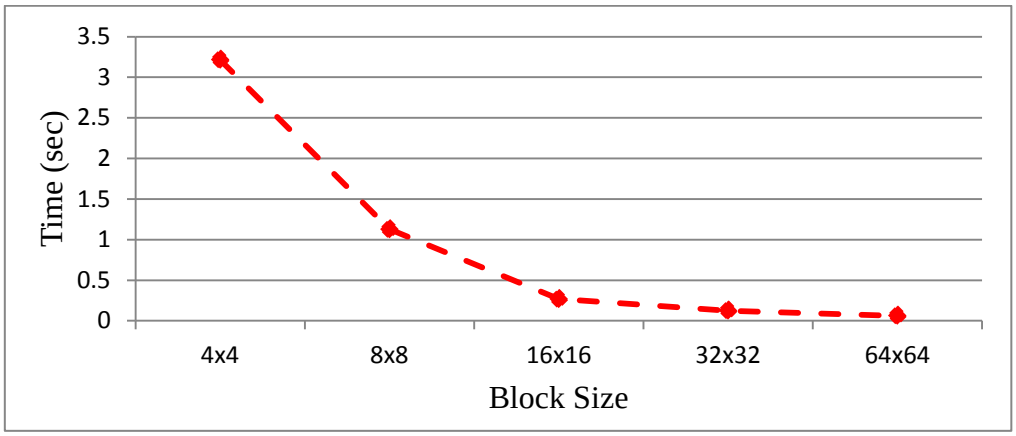


Figure 5.5: Block size vs. Generation time

From figure 5.5, it is observed that as the block size for an image decreases, the hash generation time also decreases exponentially. Therefore an optimised hash size must be chosen such that it holds important information of the image and also it must not take so long time to generate the signature that it almost becomes infeasible to implement**.**

5.1.4 Impact Of Key On Digital Signature

Key plays an important role in this proposed approach. A slightest change in the secret key can result a large variation in the digital signature generated for the same image. Here, an example of digital signatures is shown for the input image shown in figure 5.6 by applying different keys.

Figure 5.6: Input image with 256x256 pixels

Digital signature of figure 5.6 with secret key $Key1 = 112233445566$is

C85qDZsNmNGtwcze/Nz97rOdWa49AXnr23oCIX4nfauGfzptPjzROohVlX1u5SHkoN9Q2ak0a2ki3G1AQs0wZGa2rv3ETwycVs68mndIYQ5ja+IQJouLF5yZGxifTT7QA1dC4ptz8vWw4JzqEMOep8jmWLqiNRGI

Digital signature of figure 5.6 with secret key $Key2 = 912233445566$is

JFZrySl5S2Hhe2+Lg7OeDnGjCO6BttQRdqIwnv8tzAlfvprGIjU1IFpahVAcLdxFAy12ovwGL8prxyIGL61EnCTStHZG7hXpGkgJyOCROVxnTDaVRpoIhkYyfoGa6eXZgF0K/cwu+O6GBi2lbPeqmZAeLqD6ORY

One can analyse from the above data that no other person can generate the same signature without applying the same secret key, this maintains the confidentiality of the message, such that receiver can verify that the message has been signed by the expected signer only and not by some intruder.

5.1.5 COMPARISON WITH EXISTING SCHEMES

A comparison of the proposed approach with other existing techniques is shown in Table 5. 3

Table 5.3: Comparison with existing schemes

Scheme used	Original data manipulation	Size of hash/sign generated	Supports compression	Distortion in stego image
Yang and Kot [72]	Pixel flipability	Variable	Yes	Yes
Tzeng and Tsai [73]	Pixel replacement	Variable	Yes	Yes
Wu and Liu [74]	Pixel flipability	Variable	No	Yes
Yang and Kot [75]	Pixel flipability	Variable	No	Yes
Proposed scheme	No	Variable	Yes	No

Table 5.3 shows the effectiveness of the proposed approach. Less distortions and user friendly designing makes it work well for all type of applications including low budget applications where bandwidth is limited and applications where high precision is required in validating the sender without any bandwidth constraints.

5.1.6 Accuracy And Precision

Table 5.4 computations are taken for test image "Baboon" of size 512x512 pixels. It shows the impact of hash size on the RMSE values under different noise conditions.

Table 5.4: Precision analysis for variable hash length

Noise Intensity (in %)	Hash length 1	RMSE 1	Hash length 2	RMSE 2	Hash length 3	RMSE 3
10	32	130.1145	64	116.6130	128	97.7817
20	32	135.5303	64	118.6255	128	100.1082
30	32	137.9536	64	121.3681	128	102.6982
50	32	145.6484	64	124.0903	128	105.2960
70	32	151.1494	64	127.6703	128	105.4067
90	32	161.9256	64	129.9993	128	106.8237

It has been observed that for better precision, hash length must be considerably long. Noise vs. RMSE plot drawn for the above set of values is shown in figure 5.7

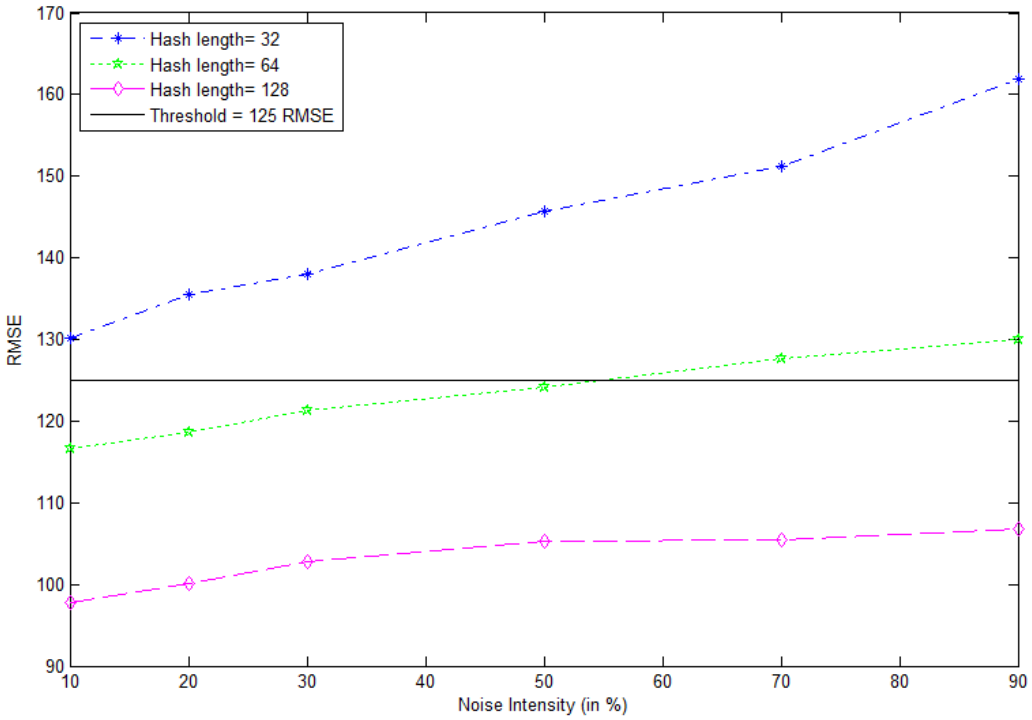


Figure 5.7: Noise vs. RMSE plot

5.2 PERFORMANCE RESULTS OF ADVANCED PROPOSED METHODOLOGY

By working on the advanced proposed approach, following results have been computed.

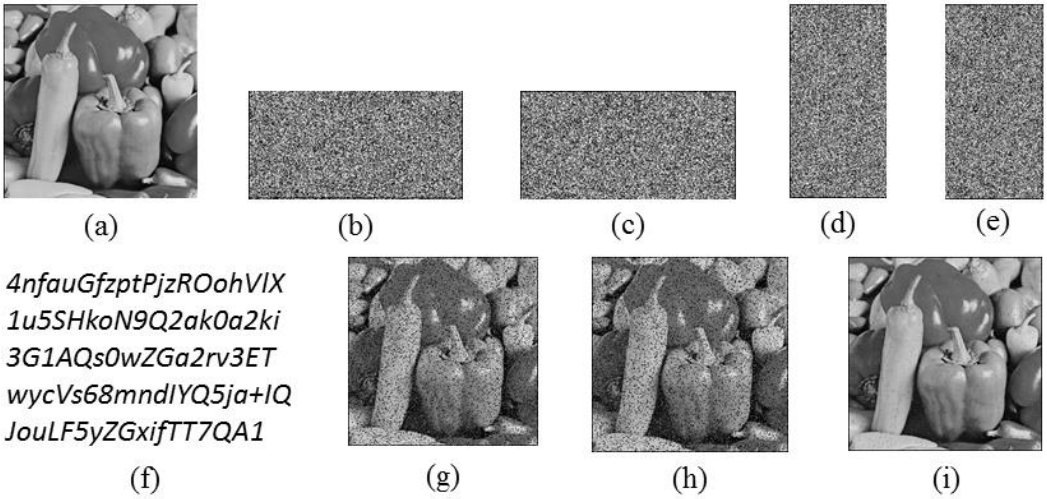


Figure 5.8: Application of advanced proposed approach on 'Peppers' Image

Figure 5.8 (a) Input image (b) Even numbered row matrix (c) Odd numbered row matrix (d) Even numbered column matrix (e) Digital signature generated for the input image (f) Odd numbered column matrix (g) Image A generated from b, c (h) Image B generated from d, e (i) Final image recovered at the receiver

5.2.1 ACCURACY AND QUALITY MEASURE

Table 5.5: Performance results of advanced proposed approach at different noise levels.

Noise Intensity (in %)	Variance (β)	Standard Deviation (σ)	Covariance (α, β)	Correlation Coefficient (ρ)
10	0.0443	0.2104	0.0421	0.9599
20	0.0399	0.1998	0.0377	0.9061
30	0.0382	0.1955	0.0353	0.8652
40	0.0356	0.1888	0.0300	0.7631
50	0.0342	0.1848	0.0247	0.7016
60	0.0333	0.1825	0.0194	0.6097
70	0.0334	0.1827	0.0148	0.5025
80	0.0336	0.1833	0.0105	0.3844

90	0.0332	0.1887	0.0046	0.2744

This advance proposed scheme results in better quality results at the receiving end. The comparison results of input image and the final recovered image at the receiver are shown in table 5.5.

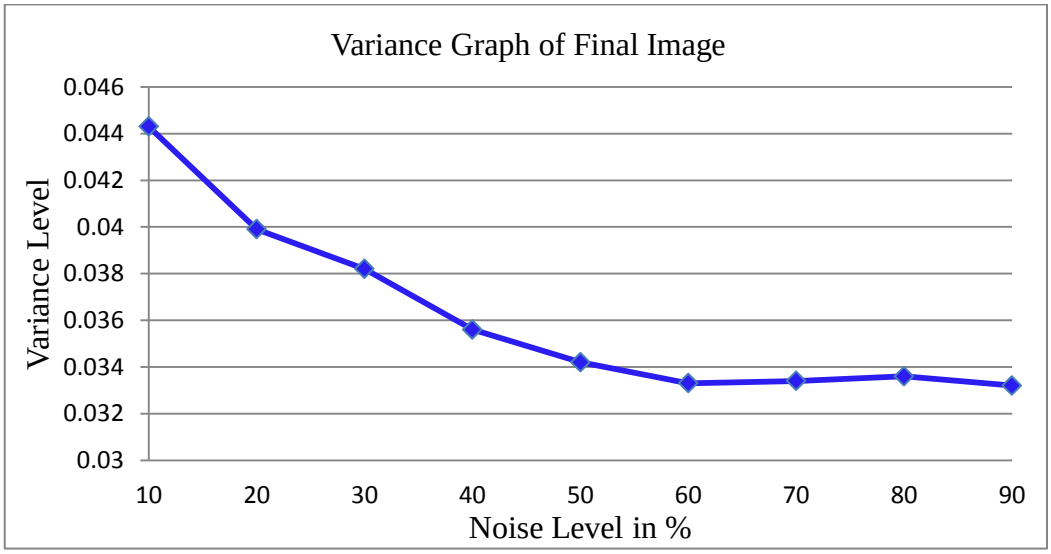


Figure 5.9: Variance plot for final image at various noise levels

Figure 5.9 shows the non-linear variations in the variance curve.

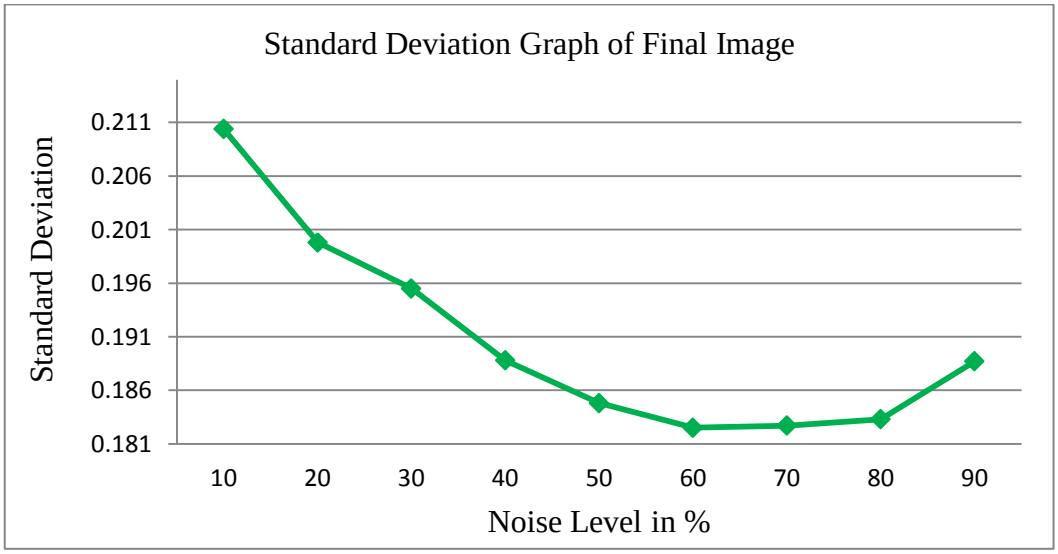


Figure 5.10: Standard Deviation graph for final image at various noise levels

Figure 5.10 represents the variation in Standard Deviation curve for final recovered image at different noise levels. As Standard Deviation is obtained from variance of same final image, therefore both the graphs have symmetry between them.

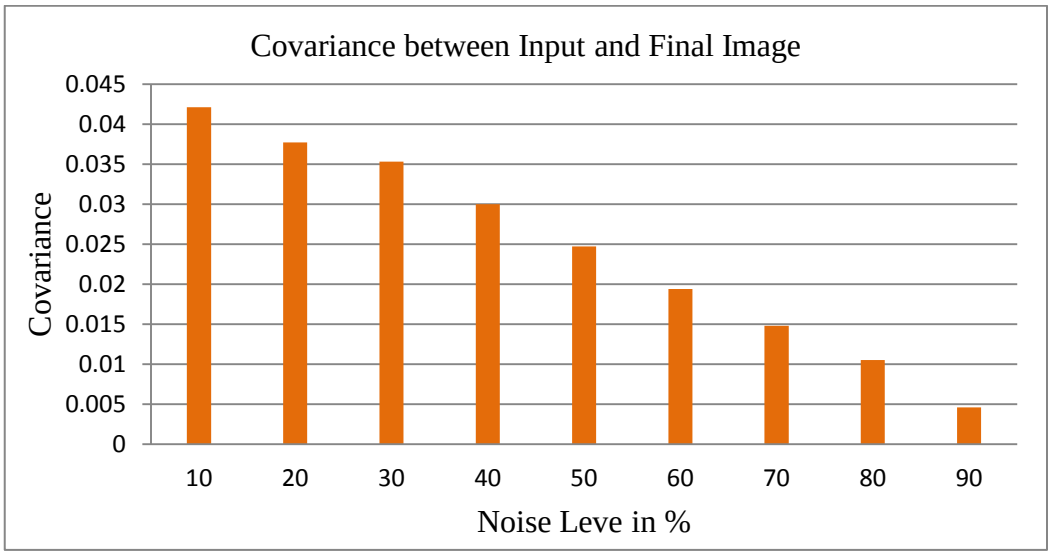


Figure 5.11: Covariance chart for different noise levels

The figure 5.5 shows the covariance levels for different noise levels. These variations are the result of difference in number of pixels that lie closer to either the lowest pixel value or extremely high value.

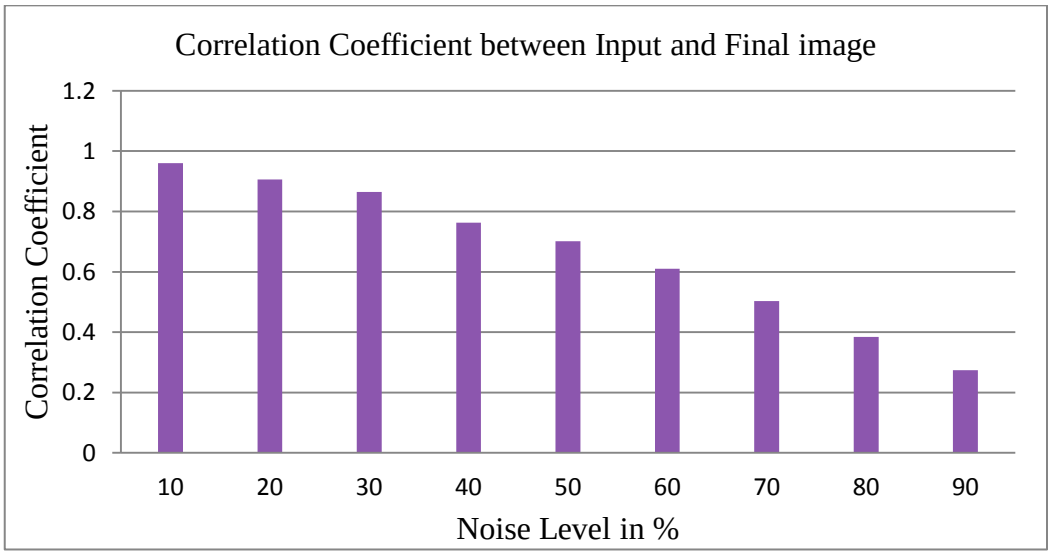


Figure 5.12: Correlation Coefficient graph

Correlation coefficient changes at each noise level. The result is shown in figure 5.12 for table 5.5. As the noise is increasing the final image generated at output becomes more and more uncorrelated with the input image.

5.2.2 TIME COMPARISON

The signature generation time for advanced proposed scheme has been compared with the earlier proposed scheme of section 4.1. Time is directly proportional to the size of the image. Larger or better the quality of image, more time it will require to generate the digital signature. Image size is taken in pixels and the signature generation time is in sec.

Table 5.6 shows the difference between time taken to generate digital signature by the simple and advanced proposed scheme.

Table 5.6: Time comparison between simple and advanced proposed scheme

Image name	**Image Size (in pixels)**	**Signature generation Time of Proposed scheme 1 (sec)**	**Signature generation Time of Advanced Proposed scheme (sec)**
Cameraman	128x128	0.0845	0.0735
Barbara	256x256	0.0921	0.1130
Lena	512x512	0.1001	0.1398
Baboon	576x576	0.1251	0.1523
Model	640x640	0.1572	0.1726
Gamer	960x960	0.1759	0.1931
Boat	1024x1024	0.1821	0.2120

The graph for the signature generation time comparison from table 5.6 is shown in figure 5.13. The advanced proposed scheme takes only a little extra time in comparison to the simpler proposed scheme, but still advanced scheme is more preferable as it provides more security.

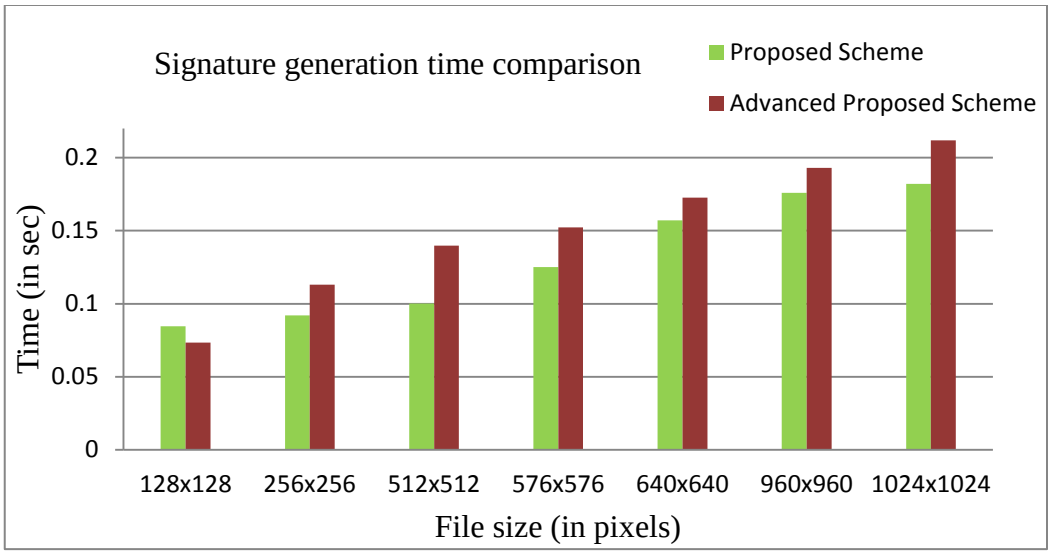


Figure 5.13: Comparison of signature generation time

It has been observed that the advanced proposed scheme takes more time to generate the digital signature. The advanced proposed scheme takes a max time of one fifth of a sec to generate a digital signature for a high quality image. Therefore both the schemes are valid for real time applications.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

Cryptography provides confidentiality, data integrity and authentication in wireless security. The properties that a digital signature must satisfy are; digital sign must be authentic, b) it cannot be forged, c) it cannot be repudiated, and d) it cannot be reused for some other user. Keeping the importance of digital signature and cryptography in wireless security, the literature survey has been carried out. Various security aspects in digital signature, cryptographic primitives and different attacks have also been critically analysed. A new approach which accurately authenticates the sender while supporting the desired modifications of image processing tools has been proposed. Flipped image has been divided into four sections which are transmitted along with digital signature. Results have been achieved using MATLAB. From the results discussed in chapter 5, it has been concluded that the proposed algorithm not only validates the sender but also supports the lossy compression techniques along with the noise offered by the transmission channel that makes it more feasible for real time applications. The variable length of hash strings is very user friendly, as it provides freedom to the users to select the hash length according to their application requirement. Optimization of bandwidth utilization has been done in order to reduce the overheads on digital signature. The basic concept of the proposed approach is clear that that main objective is to validate the sender for integrity and confidentiality of the transmitted image without wasting any resources. The efficiency of proposed work is experimentally tested under different real time problems. To achieve a high degree of precision, user can select high value of hash length. On the other hand, to make a cost effective authentication system, this same approach is used with reduced hash size and hence the bandwidth will be used in an optimised way. Evaluation of signature generation time for various images of different sizes with optimized hash length has also been achieved. The impact of key on digital signature has also been analysed. The advanced proposed approach is designed to accomplish two major aims, a) to validate or authenticate the signer, b) to provide more secure communication. Hash length has already been optimized in the simple proposed scheme to save the resources and this same hash length is used in advanced scheme. Additional security is provided by flipping the image pixels and then sending the input image via breaking it into four different planes that seems unintelligible to an unknown user. Other

advantages include fast processing; less computational complexity of the scheme also no image pixels are intentionally altered. This scheme can be applicable in unsecure environments where sender verification is important such as government sector, border security etc. As digital sign does not hold any information regarding sender's identification, therefore any unauthorized user cannot find the sender and hence privacy is maintained. Finally, the proposed schemes are compared with existing schemes of Yang and Kot, Tzeng and Tsai, Wu and Liu on the basis of original data manipulation, bit length of signature generated, and compression supportability. In future more in depth analyses can be done to use this scheme for sender identification before the processing of image. It can be done by a centralized hub that will issue certificates for registration of users to provide them unique digital signatures.

REFERENCES

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography,” CRC Press, Edition 5, October 1996.
2. Bruce Schneier, “Applied Cryptography,” John Wiley and Sons, Edition 2, January 1996.
3. William Stallings, “Cryptography and Network Security, Principles and Practice,” Pearson Prentice Hall, Pearson Education, Edition 5, June 2011.
4. Data Encryption Standard (DES), *Federal Information Processing Standards Publication, FIPS*, vol. 46, no. 3, October 1999.
5. R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*,” MIT Laboratory for Computer Science and Department of Mathematics*, vol. 21, no. 2, February 1978.
6. Marc Schneider and Shih-Fu Chang, "A robust content based digital signature for image authentication," *IEEE conference on* Image *Processing*, pp.227-230, Sep. 1996.
7. Ping Wah Wong and Nasir Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol.10, no.10, pp.1593-1601, Oct. 2001.
8. Ching-Yung Lin and Shih-Fu Chang, "Robust digital signature for multimedia authentication," *IEEE Circuits and Systems Magazine*, vol.3, no.4, pp.23-26, Jan. 2003.
9. Aloka Sinha and Kehar Singh, “A technique for image encryption using digital signature,” In *Optics Communications*, Elsevier, vol. 218, pp. 229-234, Apr. 2003.
10. Chun-Shien Lu and Hong-Yuan Mark Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," *IEEE Transactions Multimedia*, vol.5, no.2, pp.161-173, June 2003.
11. Min Wu and Liu B, “Data hiding in binary images for authentication and annotation,” *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.
12. Mehmet Utku Celik, Gaurav Sharma and A. Murat Tekalp, “Lossless Watermarking for Image Authentication: A New Framework and an Implementation,” *IEEE Transactions on Image Processing*, vol.15, no.4, pp. 1042-1049, April 2006.

13. Huijuan Yang and Kot A. C., “Binary image authentication with tampering localization by embedding cryptographic signature and block identifier,” *IEEE Signal Process. Lett.*, vol. 13, no. 12, pp. 741–744, Dec.2006.
14. Francesco Buccafurri, Gianluca Lax, “Hardening Digital Signatures against Un-trusted Signature Software,” *IEEE Transactions on Cryptography*, vol. 7, no. 2, pp. 2147-2153, May 2007.
15. Julita A., Fauziyah S., Azlina O., Mardiana B., Hazura H. and Zahariah A.M., “Online Signature Verification System*,” IEEE 5th International Colloquium on Signal Processing and its Applications*, vol. 3, no. 4, pp. 4244-4152 , March 2009.
16. S.M. Saad, "Design of a robust and secure digital signature scheme for image authentication over wireless channels," *IET Information Security*, vol.3, no.1, pp.1-8, March 2009.
17. Panagiota Lagou and Gregory Chondrokoukis, "Survey on Non-repudiation: Digital Signature versus Biometrics,” *Information Security Journal*, vol. 18, no. 14, pp. 257–266, May 2009.
18. M. O’Neill (ne´e McLoone) and M.J.B. Robshaw, “Low-cost digital signature architecture suitable or radio frequency identification tags,” *IET Computers and Digital Techniques*, vol. 4, no. 7, pp. 14–26, June 2009.
19. Lein Harn and Jian Ren, “Generalized Digital Certificate for User Authentication and Key Establishment for secure Communications,” *IEEE Transactions on wireless communications*, vol. 10, no. 7, pp. 2372-2379, July 2011.
20. Nadia M.G. AL-Saidi and Mohamad Rushdan Md Said, “Improved digital signature protocol using iterated function systems,” *International Journal of Computer Mathematics*, vol. 88, no. 17, pp. 3613–3625, November 2011.
21. Yao-Chung Lin, David Varodayan and Bernd Girod, "Image Authentication Using Distributed Source Coding," *IEEE Transactions on Image Processing*, vol.21, no.1, pp.273-283, Jan. 2012.
22. Che-Wei Lee and Wen-Hsiang Tsai, "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability," *IEEE Transactions on Image Processing*, vol.21, no.1, pp.207-218, Jan. 2012.

23. Kun Ma, Han Liang and Kaijie Wu, "Homomorphic Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack", *IEEE Transactions On Computers,* vol. 61, no. 7, pp. 1042-1049, July 2012.
24. Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, and Giovanni Puglisi, "Robust Image Alignment for Tampering Detection*," IEEE Transactions On Information Forensics And Security*, vol. 7, no. 4, Aug 2012.
25. Shiva Murthy G, Robert John D'Souza and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks," *IEEE sensors journal,* vol. 12, no. 10, pp. 2941-2949, October 2012.
26. Ajay Kakkar, M. L. Singh and P. K. Bansal, "Mathematical analysis and simulation of multiple keys and S-Boxes in a multi-node network for secure transmission," *International Journal of Computer Mathematics,* vol. 89, no. 16, pp. 2123–2142, November 2012.
27. Andrew Chi-Chih Yao and Yunlei Zhao, "Online/Offline Signatures for Low-Power Devices," *IEEE Transactions On Information Forensics And Security*, Vol. 8, No. 2, February 2013.
28. Erfaneh Noroozi, Salwani Mohd Daud and Ali Sabouhi, "Secure Digital Signature Schemes Based on Hash Functions," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 2, no. 4, pp. 2278-3075, March 2013.
29. SK Hafizul Islam and G.P. Biswas, "Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography," *International Journal of Computer Mathematics*, vol. 90, no. 11, pp. 2244–2258, April 2013.
30. Manjot Bhatia, Sunil Kumar Muttoo, M. P. S. Bhatia, "Secure Group Communication with Hidden Group Key," *Taylor and Francis Information Security Journal,* vol. 22, pp. 21-34, May 2013.
31. William Stallings, "Digital Signature Algorithms*," International Journal of Cryptologia*, vol. 37, no. 4, pp. 311–327, June 2013.
32. S. Rashidi, A. Fallah and F. Towhidkhah, "Similarity Evaluation of Online Signatures Based On Modified Dynamic Time Warping," *Applied Artificial Intelligence: An International Journal,* vol. 27, no. 5, pp. 599–617, Aug 2013.

33. Othman o-khalifa, Md. Khorshed Alam and Aisha Hassan Abdalla, " An Evaluation on Offline Signature Verification using Artificial Neural Network Approach," *International Conference On Computing, Electrical And Electronic Engineering (ICCEEE)*, vol. 3, no. 8, pp. 213-217, Oct 2013.
34. Kazi Md. Rokibul Alam1, Saifuddin Mahmud2 and Mohammad Nazmul Alam Khan, "A Comparison between Traceable and Untraceable Blind Signature Schemes through Simulation," *Informatics, Electronics & Vision (ICIEV),* vol. 11, no. 7, pp. 116-120, Dec 2013.
35. Angela Piper and Reihaneh Safavi-Naini, "Scalable fragile watermarking for image authentication," *IET Information Security*, vol.7, no.4, pp.300-311, Dec. 2013.
36. Rouzbeh Behnia, Swee-Huay Heng and Che-Sheng Gan, "An efficient certificateless undeniable signature scheme," *International Journal of Computer Mathematics*, vol. l. 92, no. 7, pp. 1313–1328, March 2014.
37. Ashok K. Bhateja, Santanu Chaudhury and P. K. Saxena, "A Robust Online Signature based Cryptosystem," 14th International Conference on Frontiers in Handwriting Recognition, vol. 13, no. 7, pp. 123-129, April 2014.
38. George S. Eskander, Robert Sabourin, Eric Granger, "A bio-cryptographic system based on offline signature images," *Elsevier Information Sciences Journal*, vol. 2590, no. 5 pp. 170-191, June 2014.
39. Tatsuaki Okamoto and Katsuyuki Takashima, "Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 409-421, Oct. 2014.
40. Xinyi Huang, Yang Xiang, Jianying Zhou, and Li Xu, "Robust Multi-Factor Authentication for Fragile Communications," *IEEE Transactions On Dependable And Secure Computing*, vol. 11, no. 6, pp. 568-581, Nov 2014.
41. Andrey Larchikov, Sergey Panasenko, Alexander V. Pimenov and Petr Timofeev, "Combining RFID-Based Physical Access Control Systems with Digital Signature Systems to Increase Their Security," *IET Computers and Digital Techniques*, vol. 6, no. 9, pp. 18-22, Nov 2014

42. Gianluca Lax, Francesco Buccafurri and Gianluca Caminiti, “Digital Document Signing: Vulnerabilities and Solutions”, Information Security Journal, vol. 3, no. 6, pp. 1-14, Feb 2015.
43. Xu Li, Xingming Sun and Quansheng Liu, "Image Integrity Authentication Scheme Based on Fixed Point Theory," *IEEE Transactions on Image Processing*, vol.24, no.2, pp.632-645, Feb. 2015.
44. Gwoboa Horng, “Accelerating DSA Signature Generation,” Taylor and Francis Cryptologia, vol. 39, pp. 121-125, April 2015.
45. Qiong Huang, Duncan S. Wong and Willy Susilo, “How to protect privacy in Optimistic Fair Exchange of digital signatures,” *Elsevier Information Sciences Journal*, vol. 12, no. 5 pp. 300-315, June 2015.
46. Mohamed F. Haroun and T. Aaron Gulliver, “Secret Key Generation Using Chaotic Signals Over Frequency Selective Fading Channels*,” IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1764-1775, Aug. 2015.
47. M. H. Jalalzai, W. B. Shahid and M. M. W. Iqbal, “DNS Security Challenges and Best Practices to Deploy Secure DNS with Digital Signatures,” Proceedings of 12th IEEE International Bhurban conference on Applied Sciences & Technology (IBCAST), pp. 280-285, Dec 2015.
48. Shannon C.E., “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no.4, pp. 656-715, Mar 1949.
49. Chaum D., “Designed confirmer signatures, Advance in Cryptology: Eurocrypt ’94,” *Springer Verlag*, vol. 50, pp. 86-91, Apr 1995.
50. Diffie W. and Hellman M., “New directions in Cryptography,” *IEEE Transaction Information Theory,*vol. 31, no. 4, pp. 644-654, June 1976.
51. Diffie W., “The first ten years of Public Key Cryptography, In Contemporary Cryptology: *IEEE Press The Science of Information Integrity*, vol. 7, no. 2, pp 135-175, Jan 1988.
52. ElGamel T., “A PKC and a signature scheme based on discrete logarithm,” *IEEE transaction on information theory*, vol. 31, no. 1, pp. 469-472, Sep 1985.
53. Fiat A. and Shamir A., “How to prove yourself, Practical solution to identification and signature problem, Advances in Cryptology : Crypto ’86,” *Springer and Verlag*, vol.

263, pp. 186-194, Dec 1986.

54. Ruland.C., "Realizing digital signature with one-way Hash function," *Cryptologia*, vol. 17, no. 3, pp. 285-300, Feb 1993
55. Merker R. C., "A digital signature based on convential encryption function, Advance in Cryptology: Crypto '87," *Springer and Verlag*, vol.293, pp.369-378, Oct 1987.
56. NIST, "Digital signature standard," *U.S Department of Commerence*, vol.186, Nov 1994.
57. Hwang T., Li C. and lee N., "Remark on the threshold RSA signature scheme, Advance in Cryptology: Crypto '93," Springer and Verlag, pp. 413-419, Feb 1993.
58. Ohta K. and Okamoto T., "A digital multi-signature scheme based on Fiat- Shamir scheme, Advance in Cryptology: Asiacrypt '91," *Springer and Verlag*, vol. 470, pp. 75 – 79, May 1991.
59. Harn L., "(t,n)Threshold signature and digital multi-signature," *Proceeding of Workshop on Cryptography and data security, Chung Cheng Institute of technology, ROC*, vol. 4, pp. 61 – 73, Mar 1993.
60. Harn L., "Group oriented (t, n) threshold signature scheme and digital multi-signature," *IEEE Proceedings on computer digit technology*, vol.141, no.5, pp. 307-313, Feb 1994.
61. Hwang T. and Chen C.C.," A new proxy multi-signature signature scheme," *International Workshop on Cryptography and Network Security, Taipei*, vol.41, pp. 26 – 28, Aug 2001.
62. Okamoto T., "A digital Multi-signature scheme using bijective PKC," *ACM transactions on computer systems*, vol.6, no.8, pp. 432-441, Nov 1988.
63. Itakura K. and Nakamura K., "A public key cryptosystem, suitable for digital multisignatures," *NEC Research and Develop*, pp.1- 8, July 1983.
64. Chaum D., "Group signatures, Advance in Cryptology: Eurocrypt '91," *Springer Verlag*, vol. 26, pp. 257-265, Oct 1991.
65. Chen L. and Pederson T.P., "New group signature signatures, Advance in Cryptology: Eurocrypt '94," *Springer Verlag*, vol. 421, pp.171-181, Jan 1994.
66. Desmedt Y., "Society and group oriented cryptography, Advances in Cryptology: Crypto '87," *Springer Verlag*, vol. 201, pp. 120 – 127, Mar 1988.
67. Chaum D. and Van Autwerpan H.,"Undeniable signatures, Advance in Cryptology:

Eurocrypt ’89,” Springer Verlag, pp. 212-216, Nov 1989.

68. Chaum D., “Zero knowledge undeniable signatures, Advance in Cryptology: Eurocrypt ’90,” *Springer Verlag*, vol. 473, pp. 458-464, Apr 1990.
69. Harn L. and Yang S., “Group oriented undeniable signature scheme without the assistance of a mutually trusted party, Advance in Cryptology: Auscrypt ’92,” *Springer and Verlag*, vol. 342, pp. 133-142, July 1992.
70. D. Kahn, *The Codebreakers: The story of secret writing*. 2nd ed. Scribners, 1996.
71. Der-Chyuan Lou and Jiang-Lung Liu, “Fault resilient and compression tolerant digital signature for image authentication,” *IEEE Transactions on Consumer Electronics*, vol.46, no.1, pp.31-39, Feb 2000.
72. Huijuan Yang and Alex C. Kot, Binary Image Authentication with Tampering Localization by Embedding Cryptographic Signature and Block Identifier, In *Signal Processing Letters, IEEE*, vol.13, pp. 741-744, Apr. 2006.
73. Chih-Hsuan Tzeng and Wen-Hsiang Tsai, “A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement,” *IEEE Communication Letters*, vol. 7, no. 9, pp. 443–445, Sep. 2003.
74. Min Wu and Liu B, Data hiding in binary images for authentication and annotation, In *Transactions on Multimedia, IEEE*, vol. 6, pp. 528–538, Jan. 2004.
75. Huijuan Yang and Kot A. C, “Pattern-based data hiding for binary images authentication by connectivity-preserving,” *IEEE Transaction Multimedia*, vol. 9, no. 3, pp. 475–486, Apr. 2007.
76. M. Hwang, C. Lee, and Y. Lai,”An untraceable blind signature scheme,” in *IEICE Trans. Fundamentals*, vol. 86−91, no. 7, pp. 1902−1906, Jan. 2003.
77. D. Chaum, “Blind signatures system,” *Advances in Cryptology*, CRYPTO’83, pp. 153−156, Feb. 1983.
78. S. Duan, “Certificateless undeniable signature scheme,” *Information Science*, vol. 178, no. 3, pp. 742–755, Mar. 2008

LIST OF PUBLICATIONS

- Harpreet Kaur, Manpreet Singh, and Ajay Kakkar, "Digital Signature Verification Scheme for Image Authentication," *2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, Chandigarh pp. 1-5, 2015.
- Harpreet Kaur, Manjinder Singh, Manpreet Singh, and Ajay Kakkar, "Image Authentication Scheme based on Digital Signatures," *Elsevier Journal on Computer Standards and Interfaces*, 2016 (communicated)
- Manjinder Singh, Harpreet Kaur, Manpreet Singh, and Ajay Kakkar, "Gray Code Image Encryption using Knight Tour Scrambler," *Elsevier Journal on Computer Standards and Interfaces*, 2016 (communicated)

801463010.pdf

ORIGINALITY REPORT

16%	9%	12%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to British Institute of Technology and E-commerce Student Paper	2%
2	apollo4.bournemouth.ac.uk Internet Source	1%
3	www.lazarusalliance.com Internet Source	<1%
4	Lecture Notes in Computer Science, 1990. Publication	<1%
5	www.irjcsea.org Internet Source	<1%
6	Submitted to Chandigarh University Student Paper	<1%
7	www.security-science.com Internet Source	<1%
8	www.ijitee.org Internet Source	<1%
9	www.kuet.ac.bd	