A Multilevel Hybrid Chaotic Cryptosystem and Authentication Algorithm for Digital Images

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Technology

in

Computer Science and Applications

Submitted By

Vinay Kumar Verma

Roll No. 601303030

Under the supervision of:

Dr. Singara Singh Kasana

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

JUNE 2015

CERTIFICATE

I hereby certify that the work presented in the thesis and as entitled, "A multilevel Hybrid Chaotic Cryptosystem and Authentication Algorithm for Digital Images", in partial fulfillment of the requirements for the award of degree of Master of Technology in *Computer Science and Application* submitted in Computer Science and Engineering Department, Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Singara Singh Kasana* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Vinay Kumar Verma)
Regn. No: 601303030

This is to certify that the above statements made by the candidate are correct and true to the best of my knowledge.

29/6/15
(Dr.Singara Singh Kasana)
Assistant Professor, CSED

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

First of all, I would like to thank the Almighty, who has guided me always to work on the right path of the life.

This work would not have been possible without the encouragement and able guidance of my supervisor **Dr. Singara Singh Kasana**. I thank my supervisor for their time, patience, discussions and valuable comments. Their enthusiasm and optimism made this experience both rewarding and enjoyable.

I am also grateful to **Dr. Deepak Garg**, Head, Computer Science and Engineering Department, Thapar University, a nice person, an excellent teacher and a well – credited researcher, who always encouraged me to keep going with work and always advised me with his invaluable suggestions.

I would like to thank **Dr. S. S. Bhatia,** Professor and Dean of Academic Affairs, Thapar University, Patiala, for giving provisions of the entire required infrastructure such as computer labs, library facilities, immensely useful for learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my family whom I dearly miss and without their blessings, this work would have been possible. To my parents, I own thanks for their wonderful love and encouragement. I would also like to thank my brother, since he insisted that I should do so. I would also like to thank my close friends for their constant support.

Date: June, 2015

Place: Thapar University, Patiala

(Vinay Kumar Verma)

ABSTRACT

In this thesis, a multilevel hybrid chaotic cryptographic system for digital images is proposed. It is basically combination of public and private keys or hybrid technique to encrypt the image. Plain and secret images are encrypted using *RSA* algorithm using *p* and *q* rounds of execution respectively. Cipher images are generated using *XOR* operations on encrypted plain and secret images. To show the effectiveness of the proposed system, *NPCR* and *UACI* metric have been calculated for five text images for five rounds. In each round, public key encryption is applied in the form of *RSA*. Due to some iteration applied on the chaotic system to obtain the cipher-image the security level will increase.

In another work, Hashing based image authentication is proposed based on the multiple transformations *i.e*. Discrete Wavelet Transform (*DWT*) with the log-polar transform. *DWT* jointly deal with all the three combination of color in an image and also it uses very less computation time with respect to other transformations. The main features of the proposed method are based on (i) the secondary image is obtained by log polar transform and (ii) the addition of images that are formed by log polar transform with the output of the *DWT* applied on the image after pre-processing. The final hash image is generated by applying the Arnold transformation on the result image according to the correlation of these magnitude coefficients and is scrambled by a secret key to enhance the system security. Various results are obtained by conducting some experiments in order to analyze and identify the most appropriate parameter values of the method that has been proposed and also results show that quality of image is not much distracted in proposed method. This scheme also shows the better sensitivity when changing the little part of image.

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1. Introduction

In the digital world, people have had some important data that they want to be secrets when they transmit from one location to another location, and other people have wanted to know these secrets. These secrets may be transmitted from Internet, e-mail, instance message, WiFi and Bluetooth *etc*. For security of data, some kinds of security techniques are required. Some of them are:

i. Steganography: A process of hiding sensitive information or data message in any type of cover media like image, video *etc*.
ii. Hashing: Hashing is basically a function in which we apply mathematical formula by which we transform a variable length of message the fixed length data by using some hash function.
iii. Cryptography: Cryptography is the technique that changes readable form of data into unreadable form of data.

The motivation behind developing image cryptography techniques is to communicate securely between one organization to another organization and it can also be used for communicating members of the intelligence or military operatives or special kind of agents of countries to decode the secret data messages and then transmit it through network. The main purpose of using the cryptography was to avoid attention to transmission of encrypted information. If suspicion was raised, then the main aim for achieve the best security of the important messages, because if any hackers noted anything change in data or secret message then the observer will be want to know the encrypted data or information inside the message data.

One of the most common reasons that intruders or hacker can be able to get unauthorized access of information and then they can try to use this information for their own purpose, to harm someone, modify and attack . As the technologies are growing continuously, due to possibilities of information to be cracked or get unauthorized access are also growing and in modern digital communication need special kind of security from intruders. This is not only limited up to data, information or communication, it also applies on computer network because internet is the only way to exchange the message or to communicate.

So, providing more security to computer network is more important because most of the important data and information is transferred over the internet. The main reason to provide is to maintain the confidentiality, integrity, availability and also to stop the unauthorized access of information. This can be stopped either hiding existence of the information or keeping the information secret. Most common ways to stop this are steganography and cryptography. Both are complementary to each other and provide better security, confidentiality and authenticity. Image cryptography is very important field in the area of cryptography. As the need of privacy and security increases, need of encrypting the important information has to be going on. If any user tries to transfer their personal information or data to another person with privacy and security he or she can transfer it by using image cryptography.

1.2. Cryptography

Cryptography provides the means to store important information or transfer it on public network (like the Internet) so that it is not available to be read by any unauthorized user [8]. The field of cryptography deals with the techniques for transferring information securely. The main goal of cryptography is to provide the intended recipients of a message to receive the data securely. Cryptography is used to prevent the eavesdroppers to understanding the information. The original message is termed as plaintext. The transmitter of a secure system will convert the plaintext into encrypt text in order to hide its meaning. This meaning will be decrypted only after the correct recipient tries to access it using correct key. This transformation process produces an unreadable output called cipher-text [8]. The algorithm used to encrypt or transform the message is called cipher. The unauthenticated user also can try to access the message so the analysis must be carried out to check the cipher‘s security is satisfactory from unauthorized users or not. Cryptanalysis is the science of breaking ciphers, and cryptanalysts usually try to break the security of cryptographic systems. In transmission a cipher-text can be transmitted easily across any communications channel because of its encrypted nature. Eavesdroppers who want to have access the cipher-text will ideally be unable to read the meaning of the message. Only the intended recipient, having the valid key combination, can only decrypt the message to again retransform the plaintext and interpret.

1.2.1. History of Cryptography

i. This cryptography has been in existence about 4000 years ago with its first and limited use by the Egyptians write his life story on his tomb using this science. They used some special type of symbols instead of words and characters and this technique was called substitution method [49].

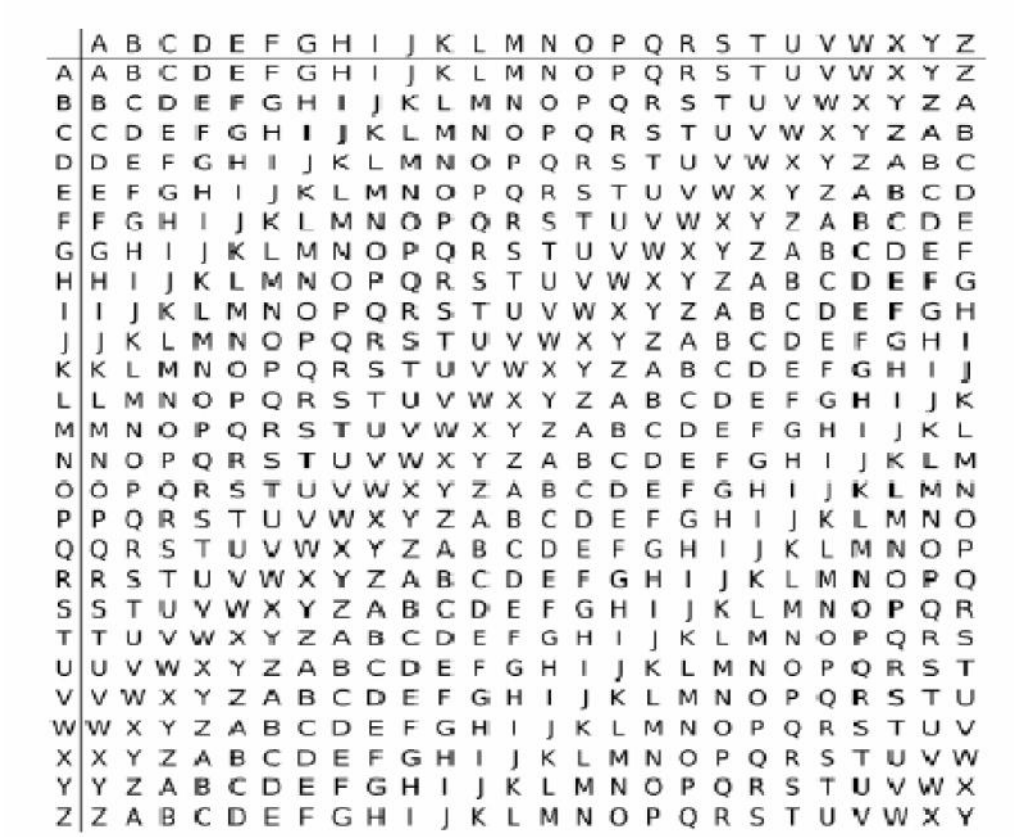
ii. Spartans developed a machine named Scytale in 500 BC. This machine or system was used a cylinder for the purpose of encrypting the personal message. The message was written in the form of cipher text on a tape in such a way so that this tape was wounded on the top of cylinder by this we can get the secret message easily [42] and this method is known as transposition method.

iii. About 2000 years ago, Roman army uses cryptography for transferring data securely. The commander of Roman army, Julius Ceasar wanted to find a solution by which they can transfer data securely or there communication was secured for that purpose a substitution method is developed by Ceasar in which a letter is replaced by another letter or symbol. In this technique, some letters can change their position and some can change by shifting some fixed length. This method was used by Ceasar during war [48].

iv. In 1500's, Bliase De Vigenere proposed a new cryptographic system which is based on Alberti's cipher disk technique. The 26 English alphabets are used as a square matrix at both aixs in Vigenere method, if someone wanted to encrypt the plain message then simply select the particular letter according to the row and column with respect to plain text and key [48] as shown in Figure 1.1.

1.2.2. The Modern Cryptography

Modern cryptography comes in the picture during last 1960's and early time of 1970's by *IBM* [14]. Data Encryption Standard *(DES)* purposed by the National Institute of Standards and Technology *(NIST),* for encoding the unidentified information from 1977. Now, *DES* was taking over by Advanced Encryption Standard *(AES),* and adopted the new standards.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1.1: Vigenere Cipher Method

Another milestone reached in 1978, when the publication of *RSA* [51] comes into the work. The *RSA* was the first end ever full public-key method that uses the pair of keys i.e. one for encrypting the plain image into cipher image and one for decrypting the cipher image back into plain image. This discovery solved the problem of key exchange in modern cryptography. *RSA* also proposed the world wide acceptable standard techniques which is also provides the authentication at receivers end and signature these techniques are authentication and electronic signatures in modern cryptography. Elliptic curves cryptography *(ECC)* [51] became popular because of its better strength over some public key cryptography such as *RSA*. *ECC* is basically produce higher security using a small size of key due to this superiority of *ECC* over *RSA* resulted into effective usage of bandwidth of channel and quick implementation of algorithm was performed [14]. This property of *ECC* made it highly useful in the field of modern cryptography. *IEEE* proposed P1363-2000 standard using *ECC* based key agreement and digital signature technique [39]. This standard contains the lists of the secured curves that can be used for

ECC based cryptosystems. These techniques require highly mathematical operations and calculations which are consuming lot of power. These cryptographic systems also have compromise on key. Chaotic cryptography was introduced in 1993; they are having advantage due to their complex behavior of their chaotic crypto systems to hide the mask information. After that, many different implementations and techniques of this technique were proposed and the different methods devised so far for the use of chaotic methods were found [51]. The chaotic behavior can be differently identified by the extreme sensitivity to initial conditions and it leads to long term unpredictability for such systems. The signals which were generated from chaotic system resulting from some chaotic dynamics are broadband and present random statistical properties of this system, although they can be generated by deterministic systems. There exists a predefined connection between behavior exhibited by chaotic systems and the properties of confusion and diffusion of the chaotic system and required for Shannon cryptosystems [51]. This cryptosystem strongly motivates the use of chaotic systems for secure communications and this system is also still questionable because of its behavior that of any chaotic function is chaotic for a finite limit. In 2005, another concept or cryptography was proposed *i.e.* policy-based cryptography. This concept gives a framework to perform cryptography operations with respect to policies formalized by Boolean monotonic expressions that were scripted in standard normal forms using Boolean expressions. An encryption policy that based encryption technique will allows us for encrypting of the data with respect to a particular scheme in such a way that only the users that having the particular scheme are able to decode the message. A policy or cryptography mainly consists of logical *AND* operation and logical *OR* operation of conditions such that each condition is consider by its digital condition that will represent the digital signature of that specific credential issuer on a certain assertion. A user compliant with a scheme only if he has been given a qualified set of keys for the scheme *i.e.* a combination of credentials that can satisfying the combination of all situation defined by the particular scheme. This scheme based encryption cryptosystem belongs to an rising family of cryptographic techniques and this policy based cryptosystems having the ability that can sharing to join together encryption with credential or key based access structures. This ability of policy based technique allows several important applications in much area but

not limited to oblivious access control [36], trust negotiation, and cryptographic order. Quantum cryptography is one of the interesting cryptography areas that will be focus in recent research of cryptography [36]. This technique is the solution of the key generation problem but the range has limited considerably. Most of the present research manly focus on the experimental result and the physics of cryptography but the force of the results could be important. Basically results shows that all present experimental activity in quantum cryptography in the quantum key exchange (*QKE*) [36]. The most experiment uses photons for generating and sharing strings of bits between two communicating parties. The security of *QKE* depends on physical law that it will not possible to extract information without knowing the disturbance about the quantum state of a particular particle. Any unauthorized client effort can be detect by the *QKE*. The security of this system does not depend on any computational and operations assumption in particular in *QKE*. The public keys pair generated by *QKE* can be never insecure due to high speed computers or new techniques are developed. In *QKE* the photons can transmitted through either by optical fibers in free space. Current experiments of cryptography shows that free space have demonstrated *QKE* over distances of the order of *20* km. In future the methodology was aimed to reach between the satellite and ground [36]. Present *QKE* technology limits using optical fibers to the distances of less than *100* km and the basic *QKE* systems using the existing telecom optical fibers that are available commercially. Present challenges in cryptography include development of some kind of system that is reliable on a single photon sources, containing higher detector efficiencies, better key generation rates, provides authentication and the integration of a *QKE* system into a computer network. Overall cryptography manly combines mathematical functions and calculations, computer science and network, sometimes electrical engineering and a different mindset that can figure out that how to get rules, break cryptography systems, and converts the designer's intentions.

1.2.3. Objectives of Cryptography

The main objective of cryptography is providing security and confidentiality but the cryptography technique used to give solution to some other difficulties [52]:

i. Confidentiality: It is about sender or receiver only can read the message information except them no one can understand the meaning of that particular message.

ii. Data integrity: Data integrity will provide a solution that the message will receive by the receiver should not be altering during the transformation through the channel.

iii. Authentication: Authentication will used by receiver to identify its origin from it will come. No other user should able to transfer a data message to receiver and vice versa. When two parties are ready to communicating with each other than they first authenticate each other to verify that the other party is trusted party or not.

iv. Non-repudiation: Non-repudiation means that after sending a message sender accepts that he send the message and should not deny that he not sends the message.

1.2.4. Encryption and Decryption

In cryptography the encryption is a transformation process that we used to information which can either applied on image, file, mail, and message and on other important documents and it transforms them into cipher text. Cipher text is a form unreadable without a correct combination of key pairs so only the intended recipient can be able to reading the data message [52].

Decryption is the reverse process encryption, which is used to converting encoded data to its original or decoded form.

A key in cryptography is basically a very long combination of bits that are used by both encryption and decryption algorithms. As the example shows, the following example will represents a hypothetical 48-bit key:

10001010 01101101 10010110 01011100 01010101 01010111

As shown in Figure 1.2, the encryption algorithm accept plaintext as the plain message and an encryption key and change the plain message by applying some mathematical operation that are based on key to create new cipher data message. On the other hand decryption process is reverse process of encryption process so it will accept the encrypted

message or cipher message as input with the same combination of key that was used in encryption process to restore the original message or the plain text.

When a user encrypts some file, another user cannot decrypt and read the file contents without the knowledge of decryption key so only the user with the decryption key can decode the cipher message to plain message. For the authentication and data integrity of the plain data message, digital signature is used. Digital signature is some kind of mathematical function that is used to validate the authentication and the data integrity [52].

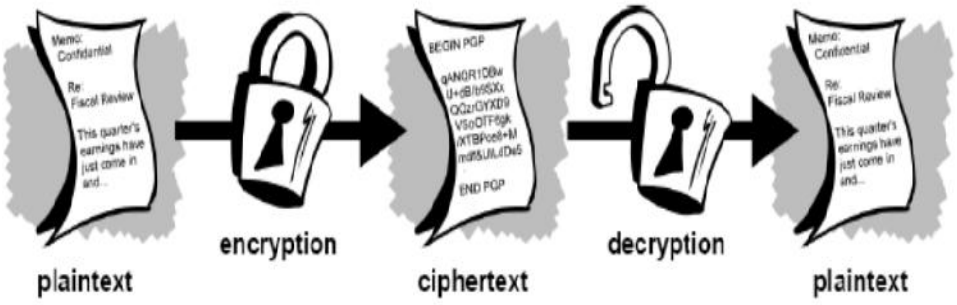


Figure 1.2: Encryption and decryption process

1.2.5. Cryptanalysis and Attacks on Cryptography

Cryptanalysis is the special art of cryptography in which decryption of encrypted message without knowing the proper combination of keys. There are many cryptanalytic techniques by which attackers can attack on the system. Some important techniques are described below for system implementer [8].

i. Cipher text-Only: Cipher text-only is the attack in which the attackers having the cipher text. This is most common type of attack but it is also difficult due to lack of important information of correct combination of key. If the attacker wants to crack that code he/she will try to apply all possible combination of keys but it will very time consuming.

ii. Known Plaintext: If we have any information then the things not harder. In known plaintext attack, the intruder having some block of simple text *x* and the corresponding cipher text message *y*. Let the example of this technique with another technique i.e. substitution cipher [8].

The below cipher text is known and is contain some information like person name "*JHONSON*" and its place called "*MIAAISSIPPI*".

YDAWPAWZYAVWGRGBWGJKKUAIJGADZEDJJDAADIID

Here, he can apply blindly the combination of keys or the frequency analysis which is not helpful for particularly on known cipher text but instead of that could decode the encrypted message using our information of the plaintext.

As we know that the plaintext contains the word *MIAAISSIPPI* so, search for a particular sequence of such 11 characters having the 3rd and 4th letters are same and 6th and 7th letters are the same and again same 9th and 10th letter having same so are the 2nd, 5th, 8th and 11th. So by matching some characters it would not take long time to notice that the sequence of words for *'EDJJDAADIID'* is the cipher text message for '*MIAAISSIPPI*' plain text message.

Same for *JHONSON*, we check for a continuous word of 7 characters where all letters are not same except for the 3rd and the 6th are same and one pair 4th and 7th are same. Regular expression is the small branch of computing studies that are useful to find the combination by matching the regular expression along with appropriate software will be helpful to search the appropriate results, but now the attacker will find that '*YDAWPAW*' will represents '*JHONSON*' With information gained so far and the cipher text based on that particular information is decrypted as shown below,

JHONSONISVWENEBWEADOUSPIESINMIAAISSIPPI

Subsequent effort of cryptanalysis will provide the complete message

JHONSON IS THE NEW HEAD OF SPIES IN MIAAISSIPPI

Here, it shows that the knowledge about the plain message providing some new possibilities of attacking into the plain text. This type of attack is feasible when some data templates are known to the others. For example, a website usually starts with some predefined text and also ends with 'Yours Sincerely' or

‘Regards’.

iii. Chosen Plaintext Attack: The chosen plain text attack is not similar from Known Plaintext Attack because in this the attacker can choose which plaintext message to be encode and after analyse the result and relationship of the output cipher text to getting the combination of keys used for encoding method. For example, we try to attack on the message that we have know so first send a mail to other party. That mail contains that particular word about us having the knowledge for example in previous example “*MIAAISSIPPI*”. So we send a mail like, “Please tell *JOY* that saying *MIAAISSIPPI* will reach in just one second”. Then *JOY* reply that mail with some encrypted form of message by which we extract some information or the exact cipher word with respect to “*MIAAISSIPPI*” and by this the key analysis also performed using some mathematical functions and calculations. The chosen plain text attack stronger as the attacker has more control of the mathematical function.

iv. Chosen Cipher text Attack: The chosen cipher text attack is similar as chosen plain text attack and mostly associated with the decoding process where the opponent having the limited access to the system where the decryption process has performed. They can choose a cipher text block to decrypt the corresponding plain message.

1.3. Types of Cryptography

Basically there are many ideas of categorized cryptograph techniques. According to my thesis, cryptography techniques are divided on the bases of no of the key used for encoding and decoding the message information and also define the use and applications of these types of cryptography [39]. The two types of cryptography techniques are given below:

i. Private/Secret Key Cryptography (*SKC*)
ii. Public Key Cryptography (*PKC*)

1.3.1. Private/Secret/Symmetric Key Cryptography

In private key crypto system one key is used for both the time i.e. encryption and decryption at sender and receiver side respectively. The sender has some key or some predefined set of rules to encode the plain message into cipher text to transmit cipher data to the receiver using any channel. The receiver receives cipher text and applies the same key or set of rule to decrypt the cipher text into the plaintext. As a single key is used for both encryption and decryption it is also known as symmetric encryption or symmetric cryptography [52].

In this type of cryptosystem, it must that the key should known to both the sender and the receiver and it should be secure. The biggest problem with this type of technique is how to distribute the key between two parties.

Private Key cryptography techniques are normally classified as stream ciphers or block ciphers. The stream ciphers apply on a byte or word at a same time and implement a kind of function by which complete plain text message will encrypt and converts into cipher text. The another type of cipher encodes one block of data message at a time by using the same key on every block of data as it is called as block cipher. In general, when we apply the same plaintext block data it will always encrypt to same cipher text data when using the same combination of keys in a block cipher whereas the same plain message encrypt to different cipher text in a stream cipher. Some most common type of private key cryptography schemes are *DES* and *AES.*

Data Encryption Standard (*DES*) [52]: *DES* is the manly secret key cryptography technique used as private key cryptography; *DES* proposed by *IBM* in the year of 1970s and adopted by the National Bureau of Standards (*NBS*) in 1977 for unclassified government applications. *DES* is belongs the category of block-cipher cryptography that using a 56-bit key which works on 64-bit block of data at same time. *DES* has some complex set of transformation rules that include complex mathematical functions that designed for specifically fast hardware implementations and at the same time slow software implementations, but due to high speed computers processors are available so this point is becoming less significant today. *IBM* also developed a scheme in which 112-bit key are used but it was rejected by the government in the 1990s.

1.3.1.1. Advantages of Private/Secret/Symmetric Key Cryptography

i. A symmetric cryptosystem is faster than public key cryptosystem.
ii. In symmetric cryptosystems, encrypted data can be transferred on any channel because the key is not transmitted with the data so there is not a possibility that the data will be intercepted.
iii. A symmetric cryptosystem also uses password authentication to prove the identity of receiver.
iv. A user only having the secret key can decrypt a message.

1.3.1.2. Disadvantages of Symmetric Key Cryptography

i. Symmetric cryptosystems have a big problem of key transportation. Before the message is being transmitted to the receiving system the key has to be transmitted. In the digital world electronic communication is insecure as it is impossible to guarantee that the message will transmitted securely or no one will be able to tap communication channels. So for the secure communication the only way of exchanging keys would be exchanging them personally.
ii. Symmetric key cryptography cannot provide digital signatures that cannot be repudiated.

1.3.2. Public/Asymmetric Key Cryptography

PKC has been the mostly used cryptography in the last few decades' of the new world of cryptography. It was first developed by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976 [15]. They proposed a pair-key crypto system in which two communicating parties could exchange of message in a secure manner over a non-secure communications channel without having to share a secret key one is for sender and other for receiver.

PKC employs two keys one is encryption key and another is decryption key and that are mathematically related to each other but information of one key from the two does not allow anyone to easily find the other key. Encryption key will be used to encrypt the plain message into cipher message and the decryption key is used to decrypt the cipher

text message to again plain text. The main thing here is that we can apply any key first, it does not matter that which key was applied first and which is second, but the main point is, both keys are required for the process the encryption completely. This approach is required a pair of keys so it also called as asymmetric cryptography.

In *PKC*, there are two keys. One is known as the public key and may be published as widely over the network. The second key is known as private key it is never known to another party. It is simple to send data under this scheme. Let us consider an example; *Jeni* wanted to send a message to *Joy*. *Jeni* encrypts some plain text information using the *Joy's* public key. *Joy* decrypts the cipher text message using his private key back into plain text message. This method also used to prove integrity of message and also provide the authentication. For example, *Jeni* could encode some plain message with her secret key and *Joy* decrypts by applying *Jeni's* public key than he knows that *Jeni* transmit the message data and *Jeni* cannot deny about having transfer the message.

1.3.2.1. Advantages of *PKC*

i. In asymmetric or public key cryptography there is no need for exchanging the keys so the key distribution problem is removed.
ii. The primary advantage is increased security of public-key cryptography, the private keys do not ever need to be transmitted or revealed to anyone.
iii. Public key cryptography can provide digital signatures that can be repudiated.

1.3.2.2. Disadvantages of *PKC*

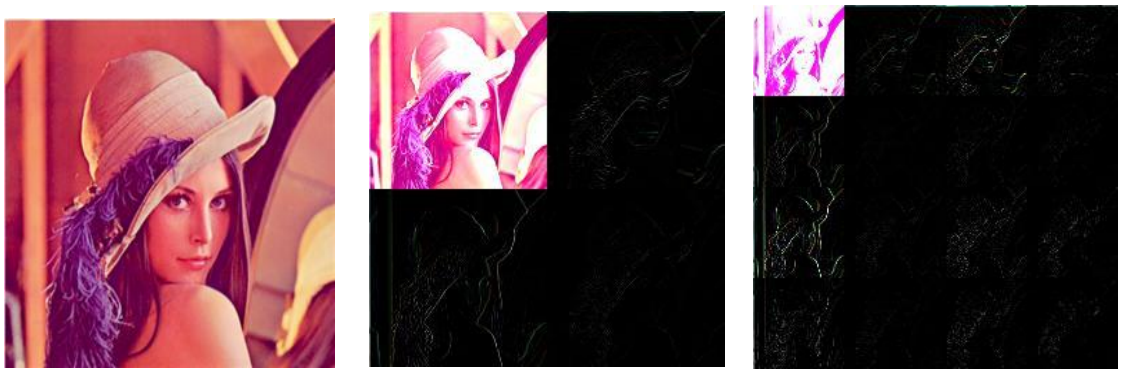
i. A disadvantage of using *PKC* is time complexity for encryption. There are some popular secret-key encryption methods present which are significantly faster than public-key encryption method.

1.4. Discrete Wavelet Transform *(DWT)*

A wavelet transform basically decompose a signal into the set of various basic functions and these various functions are known as wavelet. *DWT* transform discrete time signals into the discretely sampled known as discrete wavelet representation.

The first *DWT* invented by mathematician Hungarian Alfréd Haar. This is basically using 2^n numbers as input which is represented as a list. This wavelet transform can pair up the input values that considered for storing a difference between them and also passing the sum. The above procedure is repeated recursively for pairing the sum to provide the next level sum, which is $2^n - 1$ differences and the final sum.

The *DWT* has huge amount of uses in modern science and technology, mathematics, and engineering and computer science. Mostly, *DWT* is used for signals that is coded, to present a discrete signal in a more compressed form, often as a pre-processing for data compression some real life applications also found in many signal processing of accelerations for gait analysis in digital communications and many others. The compression algorithm of *DWT* will starts by translating image from data space to wavelet space and this is done several times or levels. Below example will start with data applying on to the two-dimensional transformation matrix and get the output image and the components are grouped into four parts, like in the Figure 1.3.



(a) (b) (c)

Figure 1.3: *DWT* 2-level results when applied on Lena image.

1.5. Outline of the Dissertation

Based on this research contribution, the dissertation is divided in the following chapters. Chapter 1 includes the introduction part of the thesis like the various types of cryptography and history of cryptography *etc.* Chapter 2 examines various research

papers that are related to cryptography and image authentication and cryptography algorithms. It discusses previous proposed works that form the roots of subsequent research in the field of cryptography and image authentication. Chapter 3 explains the proposed work based on cryptography *i.e.* A Multilevel Hybrid Chaotic Cryptosystem for Digital Images. Chapter 4 explains the proposed work based on image authentication *i.e*. Arnold Hashing for Image authentication using Multiple Transform and the last Chapter contains the conclusion and future work.

Chapter 2: Literature survey

A lot of work has been done in the area of cryptography. But security and time complexity in cryptography still a big challenge. Many researchers have given various cryptography techniques and strategies to solve this challenge.

The most common secret key cryptography technique used now a days is *DES* was introduce by *IBM* and adopted by the National Bureau of Standards for encrypting the unclassified information and some governmental applications in 1977 [51].

DES is a symmetric block cipher encryption technique that transforms 64-bit of data blocks at a time using a 56-bit shared secret key and it will consists 16 rounds of permutation and substitution steps. The overall scheme of *DES* encryption having two inputs to the encryption method *i.e.* the plaintext message to be encrypted and the key. In *DES*, the plaintext message is of 64 bits block data length and key is 56 bits long. The complete processing of the *DES* encryption consists of three phases. In the first phase, the 64-bit plaintext message passes through an initial permutation (*IP*) that are used to rearranges the bits and the result of this phase is permuted inputs. The second step is contains 16 rounds of the same function *i.e.* permutation and substitution functions in each round. The output from the last (16^{th}) round consists the 64 bits of block data that are a input to the function of plaintext and the key. The left halves and the right halves values of the output bits are swapped to produce the pre output. Now, this pre output was passed through a permutation function that is the inverse of the Initial permutation function which is performed before, to produce the 64-bit cipher-text. The 56 bit key is used in all 16 rounds of permutation function. In each 16 rounds, a sub-key is produced by the combination of a left circular shift function and a permutation function. The permutation function was the same for each 16 rounds, but in every 16 rounds a different sub-key is produced due to the repeated iteration of the key bits [52].

The internal structure of a single round consists 2 blocks. The left block and the right block of each 64-bit intermediate value are treated as separate 32-bit block data and each rounds consists some complex sequence of operations like permutations, substitutions, and the exclusive-OR (*XOR*) function.

Some security issues are there because secret key encryption algorithm uses a 56-bit key, or 7 byte long. It was believed that trying out all the combination of 72,057,594,037,927,936 possible keys would be impossible because no computer become fast enough at that time. In 1998, one organization Electronic Frontier Foundation (*EFF*) developed a special kind of machine that can decrypt a cipher message back into plain text message by trying out all possible combination keys in less than three days.

To overcome that particular problem Triple-*DES* was developed it has three 56-bit *DES* keys so the total key length is 168 bits. In first step it encrypt the plaintext using *DES* with first 56-bit key than in second step decrypt the output of first step using *DES* with second 56-bit key and in last round encrypt the output of the previous round using *DES* with last 56-bit key.

In November 2001, National Institute of Standards and Technology (*NIST*) announced the *AES* [25]. *AES* is the successor of *DES*, which cannot be considered secure any longer, because of its 56-bit key length. To determine which algorithm would better than *DES*, *NIST* compared different algorithm and best of all would become the *AES*. There are three different versions of *AES* and all of them having a block length of 128-bits data, whereas the key length is different 128, 192, or 256 bits according to need.

This method consists of 10 encryption rounds; first the 128-bit key is explored into eleven round keys having size of each key is 128. Each round includes some functions that are transforming using the corresponding encryption key to make sure the security of the encryption process [52]. After initial round of encryption, the first round key is *XOR* to the plaintext and 9 equally structured rounds follows. Each round consist some operations they are: substitute bytes, shift rows, mix columns and addround key. The last round also similar to all the rounds but the Mix columns step is omitted in this round.

Sub bytes operation is one of the nonlinear substitutions and there are many ways of performing the Sub bytes operation. In this step a lookup table is used to map the values of 16 byte state to another corresponding 16 byte using that table. The Shift rows operation processes on different rows and this function is applied on each row. A simple rotate with a different no of shift bits are performed and that no of bits are depends on the row numbers on which that particular function is applied. The second row of the 4x4 byte input data was shifted one byte position to left side in the state matrix same as the third

row is shifted two byte positions to the left side in that state matrix and so on. The first row was unchanged. The mix columns function is the more complex operation as compared to previous ones from a software implementation perspective. Mix column operation is performed on columns and each column of the state matrix can be multiplied with a fixed matrix that is predefined previously. The simplest operation in the all 4 operation is Add round key operation. The corresponding bytes of the input state matrix and the expanded key are *XOR* with each other.

In key expansion process the 128 bits of the original key are expanded into eleven new 128-bit round keys by applying the key expansion formula.

AES has many advantages but the main issue is about security while exchanging of keys due to the nature of symmetric key. So the new type of cryptography technique are comes into the picture that is public key or asymmetric key cryptography.

Diffie *et al.* [15] proposed an algorithm for key exchange between two parties. This algorithm solves the problem of sharing the key. If *Alex* and *Boby* want to share a secret key that they want to use in a symmetric encryption algorithm, but their communication channel is insecure. The attackers are observed every piece of information that they exchange. So *Alex* and *Boby* to share a key the Diffie and Hellman introduce a new algorithm without making it available to Eve.

First step is for both sender and receiver to agree on a large prime number *q* and a nonzero integer number *g* modulo *q*. now they make the values of *q* and *g* public. The second step is for sender to pick a secret integer number *a* and keep that number secret from everyone and at the same time receiver also picks an integer *b* and keep it secret. Now they calculate the *A* and *B* by using some mathematical formula as given below:

$$A \equiv g^{a} \pmod{q} \qquad B \equiv g^{b} \pmod{q}$$

Where, ≡ is mathematical equivalence operator

The next step is to exchange these computed values *A* and *B* between them through any channel so that Eve can see the values of *A* and *B*, since they are sent over the insecure communication channel. Finally, they are again uses their secret numbers to again recalculate the values A' and B' by given formula:

$$A' \equiv B^{a} \pmod{q} \qquad B' \equiv A^{b} \pmod{q}$$

The values that they compute, A' and B' respectively, are actually the same, since

$$A' \equiv B^a \equiv (gb)^a \equiv g^a \equiv (g^a)^b \equiv A^b \equiv B' (\text{mod } q).$$

Rivest *et al.* [45] proposed *RSA* algorithm for public key cryptography in 1977. The RSA system uses more complex functions; the system will use the modular function to encode information into unreadable encrypted text. This function was some time known as "clock" arithmetic, because the summation and difference are similar clock time. In a 12-hour system, 2 hours after 11:00 is not 13:00 (11 + 2 is not equal to 13); it is 1:00. This is because we subtract out 12 (or any multiples of 12) after doing the addition. In modular arithmetic the function are performed like given below:

$$1 = (11+2) \bmod 12$$

$$1 = 13 \bmod 12$$

The multiplication in modular arithmetic is same as the addition is done in above equations.

$$6 = (9 \times 2) \bmod 12$$

$$6 = 18 \bmod 12$$

The *RSA* system uses multiplication modular arithmetic function instead of multiplying one number by another number, The *RSA* system multiplies one number by itself a number of times that the second number. So the first number that is multiplied by it is called the base and the second number that much time the number is multiplied is called the exponent.

$$81 = 3 \times 3 \times 3 \times 3$$

$$81 = 3^4$$

In this example, the number (3) is the base, and is multiplied by itself four times, making the exponent the number (4).

In the *RSA* encryption scheme the message *M* is multiplied by itself *e* times so that the product is similar to the *M* to the power *e* and then the modular function is applied to that particular result so now the new result is cipher text as *C*.

$$C = M^e \, m \quad n$$

This function is very hard to recover the message *M* again from the cipher text *C* when *n* is a very large number like *200* digits. Even faster computer cannot compute such functions in reverse order. So for decryption process the different parameters are used. In the decryption process, a different exponent number *d* is used to convert the cipher text back into the original message plain text *M*:

$$M = C^d \, m \quad n$$

The modulus number *n* is a composite number and it obtained by multiplying two large prime numbers *p* and *q*

$$n = p \times q$$

The encryption and decryption function values are related to each other

$$d = e^{-1} \bmod ((p-1)(q-1))$$

To calculate the decryption key, from the prime numbers *p* and *q* we must know the one of the value. The *RSA* Algorithm can be divided into three simple steps. First is key generation, in which the key is generated from the 2 large prime numbers. Second step is encryption, in which the message *M* is converted to the cipher text message *C* using the encryption key and the plain text message. Last step is decryption process, in which the cipher text *C* is decrypted back again into the plain text message *M* using the decryption key and the cipher text message *C*.

Denning [13] proposed a digital signature algorithm or technique by which a message is authenticated. It proves that a message is coming from an authenticated sender, similar to the signature on a paper document. Sender first encrypts the message with his private key so that receiver can decrypt that using the common combination of the key because that public key is available publicly. So it is verified that the message is from only sender from it expects.

The development of digital signatures we have to goes back in the public key cryptography. Diffie and Hellman proposed an idea by which the every user can verify the message contains but no one can change and generate the message [15]. They proposed a generic function for digital signatures that solves a problem of authentication. The method proposed by Rivest, Shamir, and Adleman in 1977, called as "*RSA*," [45] become the very popular, and used in many areas for security. Two more techniques, first

is discrete logarithm that contains Digital Signature and the Diffie-Hellman's concept of key exchange scheme and second is elliptic curve method [1] are also used in many fields but not as compared to *RSA*.

The *RSA* digital signature algorithm provides the security as well as digital signature on the same time so the authentication and privacy both are applied at the same time using this scheme. The sender's private key is used to generate a signature (as shown in Figure 2.1) so that the message is signed by sender. The second step is to encrypt this by using receivers' public key so the message is both signed and encrypted. Now this cipher message can be transmitted to the any insecure network. Receiver can receive the cipher message and then first apply the secret key to decode the data and then apply the sender's public key so that the authentication of the message is done successfully.

Any signature generated by the first function from the sender side has always identified correctly and the second operations at receiver end if and only if the key used that are public key. If the two signatures are different it means that the information was altered or the message is from false user so we can ignore the message.

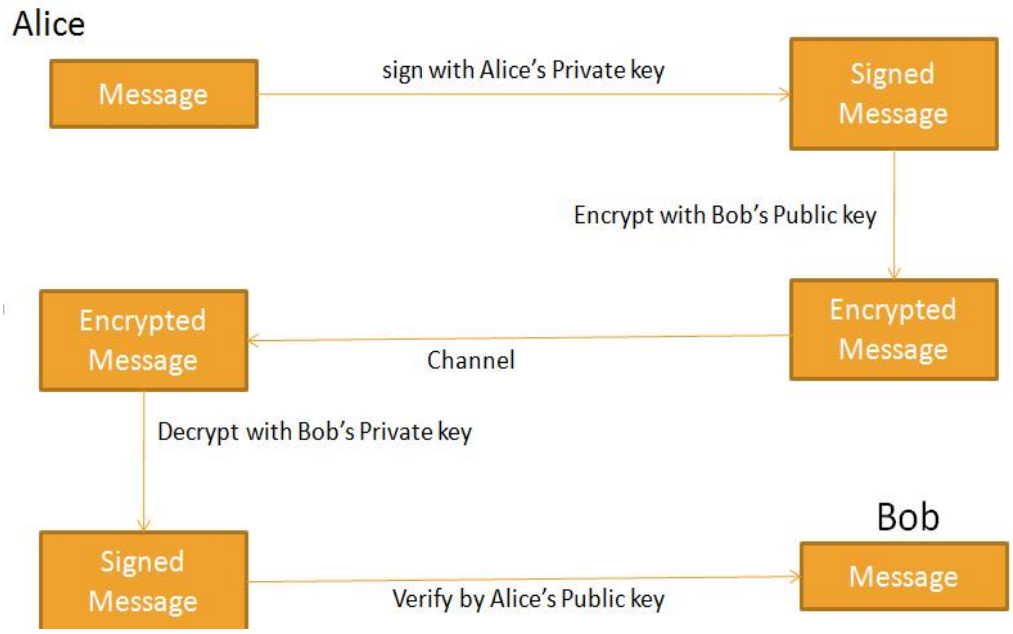


Figure 2.1: Digital signatures with RSA

ElGamal [16] proposed a cryptographic system in 1985 which is a version of the Diffie-Hellman key distribution algorithm and it will also allow secure exchange of messages between the sender and the receiver. ElGamal cryptosystem mainly contains three main parts that are: first is key generator, second is encryption algorithm and last is decryption algorithm. In key generation first select a prime number q that should be large and another number g that primitive element of mod p. Now the sender selects its private number x that is used to calculate key as $y = g^x \ mod \ q$. The second step was the encryption for that sender selects a random number k and calculates the key for message by: $K = y^k \ mod \ q$ than calculates cipher text pair $P = \{P1, P2\}$ as:

$$P1 = g^k \ m \quad q$$

$$P2 = K \times M \ m \quad q$$

This cipher text is then forward to the recipient and the value of k should be destroyed after use and never used again. The final step is decryption for that the key is formed by receiver by the formula: $K = P_1^x \ mod \ q = g^{k.x} \ mod \ q$ and than extracts plain text message M by equation: $M = P_2.K^{-1} \ mod \ q$. The only disadvantage of using this type of system is that it would double the size of data to be transmitted. So it is totally wastage of time and memory.

2.1. Literature Related to Chaotic Cryptography

Today is the digital world, the use of computers and computer in the field of networks grown very vastly. New network are used to connect many people using the global internet that are used worldwide. Today, the message transmitted through these networks are not just only data, but contain multimedia data like images, video and audio data etc. Some conventional cryptosystem directly encrypt image data. But this is not advisable because of their large size of data and real time constraints of image data. Conventional cryptosystem require a lot of time to direct encrypt thousands of image pixel values. On the other hands, unlike textual data, a decrypted image is usually acceptable even if it contain small level of distortion [50]. For all the above mentioned reasons, the algorithms that function well for simple data like text files may not be used for other types of data like images and videos. Many studies have been performed on the use of textual

encryption algorithms for images by modifying the algorithms to adapt with image characteristics. One such option for encrypting an image was to consider the two dimensional array of image pixels value as one dimensional stream of data and then to encode the data block with any conventional encryption method [22].

Many works in the area of image cryptography has been done. But security and time complexity in image cryptography still a big challenge. Many researchers have given various image cryptography techniques and strategies.

The first chaos-based cryptosystem was proposed by Matthews in 1989 [40]. Subsequently, the amount of research on chaotic cryptography increased rapidly, while trying to break (and find the weakness of) the proposed schemes in order to improve chaos-based cryptosystems.

Wang *et al*. [61] proposed the algorithm for encrypting color images using a logistic map but it was not success and it was broken by Li *et al*. [34]. Another technique was designed by Li *et al*. [33] that was the recent work of Zhu [70]. He applied hyper chaotic sequences to generate the key stream of bit sequence but Li in his work proved that the proposed algorithm by Zhu was not sufficiently robust against a chosen plaintext attack. Wang *et al.* [62] was proposed another cryptosystem that is the combination of the Lorenz map and perceptron model of the neural network but it was also not sufficient against chosen plain text attack. This chaotic cryptosystem or algorithm was cracked by Zhang *et al*. [68] after analyzing its security against plain text attacks. The experimental results show that the secret key can be reconstructed using one pair of known-plaintext/cipher text attacks. Furthermore, the effect of changing one bit in the plain image is a change only one bit in encrypted image at the same position. Many similar works have failed in security analysis.

Hence, according to above points when designing and implementing a chaos-based cryptographic encryption system, some requirements should be kept in mind these are most important.

Alvarez and Li [4] proposed a common framework for chaos based cryptosystem and it will consists three main points they are implementation rules, key management tips, and security analysis approaches. According to these basic guidelines guarantees an acceptable level of security with the chaos-based cryptosystem scheme. Moreover,

Alvarez and Li in [3] proposed a practical security analysis scheme of a cryptosystem which is providing security agents chosen plain text attacks based on the Baker map. In addition to cracking this cryptosystem due to vulnerability of the key, some countermeasures are introduced for improving and enhancing the security of these types of cryptosystems. Alvarez and Li [4] another cryptanalysis algorithm presented that the algorithm given by Gao *et al*. [22] that is nonlinear chaotic algorithm is not secure according to failure in the plain text attack and statistical and key space analysis.

Chaos-based encryption cryptosystems are based on diverse types of chaotic maps and also on discrete maps. Most of these algorithms or cryptosystems are a combination of two or more chaotic maps to achieve a better complexity, security, and expanded key space.

Guan *et al*. [23] proposed a combination of the Arnold cat map and the Chen map in this the Arnold cat map was applied to clutter the position of the pixels and then applied *XOR* with the discrete output signal of the Chen map to modify the gray value of the cluttered pixels. Xiao *et al.* [66] was analyzed and improved this by finding the weakness of the proposed algorithm or the cryptosystem and they also overcame the flaws.

Fu *et al*. [21] proposed a novel shuffling algorithm to overcome the disadvantages of permutation-only cryptosystems, this algorithm or cryptosystem performs an efficient bit-level permutation in two stages of chaotic sequence sorting and Arnold cat map.

Their analysis and results show that this encryption technique for security is more secure and has much lower computational complexity than compared to previous similar works.

Xu *et al*. [67] was analyzed the improved cryptosystem of Xiang *et al*. [65] and found two drawbacks. In their proposed work, iterating Chen chaotic system generates the random number sequence, which is more random as comparison with the sequence of number that was generated by logistic map cryptosystem in [65]. The another drawback is overcome by arranging the parameters of Chen map using only the last one byte of encrypted plaintext after every iteration, that raise to a higher sensitivity of encrypted image as compared to the plain image. This technique was fast according to simulation results and secure according to large size of key space.

Fouda *et al*. [19] was proposed a block cipher cryptosystem to overcome the drawback of time-consuming real number arithmetic calculations that was found in chaos-based image

encryption techniques. This relatively fast and more secure chaotic scheme is based on sorting the integer coefficients of linear Diophantine equation (*LDE*), which is generated dynamically by only two rounds any of chaos maps.

Chen *et al*. [11] is proposed another work that enhances the efficiency of chaos-based encryption cryptosystem. They found permutation-diffusion encryption techniques are designed with very high computation of at least two chaotic maps and weak against known/chosen plaintext attacks. Hence, they generate the state variables from the 3D or hyper chaotic maps by designing a dynamic mechanism for snake-like diffusion and pixel-swapping confusion. A tiny change (e.g., one pixel) will generate a totally different sequence of key bit stream at the first round of encryption.

2.2. Literature Related to Image Authentication

With the wide use of various image editing tools, image contents can be easily tampered or modified. Verifying and image authentication are therefore a major issue in many applications of image transmission. Arnold image hashing is widely applied in image authentication [2, 30, 69]. Basically, image hashing methods can extract important features of image from which a short binary or real number sequence and it is called hash and is generated to represent the image content. Such type of hash function should be robust to image content preserving operations while being sensitive to various malicious tampering attacks. Because arnold image hashing method captures the main image characteristics and it has also used in other applications like image forensic [37, 6], image retrieval [32, 71], digital watermarking [20, 9], and so on. Considering image authentication, an arnold image hash function should also have good anti collision capability for visually distinct images and also a satisfactory level of security in order to make very difficult for an adversary to forge the hash value from hash function. To meet all the requirements for construction of the robust image hashing is still a challenging task.

In general, the construction of an image hashing is based on three basic steps, *i.e*., pre-processing, feature extraction of image and construction of hash function. From all of them, the most critical factor is image feature extraction step [53]. The feature extraction methods for image hashing are classified into the following categories.

Discrete Cosine Transform (*DCT*):- some image hashing methods like Fridrich and Goljan [20] used the *DCT* transformation to capture the essential or important features of image blocks. In both the functions they observed that it is really difficult to change the correlation of the low frequency *DCT* coefficients of image without attacking or tampering on the content of an image. Therefore, the low frequency *DCT* coefficients of image can be used as features to build the hash function. De. Roover *et al.* [46] defined a vector *i.e.* radial variance vector (*RAV*) and it basically focus about the radial projection of image pixels. According to this applied the *DCT* to compress the *RAV* feature vector of pixels of the image and construct the image hash function. This scheme is more robust for content preserving functions and small angle rotations in images.

Discrete wavelet transform (*DWT*):- Ahmed *et al*. [2] uses wavelet transform to extract the important image features and the wavelet transform has a good time frequency technique, their function can locate and tampered regions with a good accuracy in the image data but at the price of a longer image hash. Wu et al. [63] combined the Radon transform method (*RT*) with the *DWT* to solve the problem of print scan attacks. Tang *et al*. [55] proposed an image hashing method when he observing that the entropy of pixel blocks after content preserving operations, a measure used to characterize image texture is the approximately linearly changed after content preserving operations. Then, according to this method they applied *DWT* to image block's entropies to analyze the feature compression and construct of the image hashing. Recently, color vector angle combined with *DWT* [54] were proposed, according to robust image hashing, their results and analysis show good robustness and randomness to common content preserving operations and small angle rotation. Liu *et al*. [31] in his method utilized the wave atom transform to extract the main image features arguing that this approach has a sparse expansion of the image and is capable to better capture texture properties for randomness. Furthermore, they analyze that the coefficients of the third scale band are more suitable and correct for serving as image hash features as compared to other scale bands.

Discrete Fourier Transforms (*DFT*):- *DFT* based transforms are executed very quickly. Most of *DFT* based techniques are mixed with other transforms in order to prevent from geometric distortions. Swaminathan *et al*. [53] proposed a robust image hashing

technique which is basically based on the Fourier Mellin transform. Qin *et al.* [44] proposed another technique in which a secondary image is obtained first after a rotation projection similar to the *RAV* of the image. After that a non-uniform sampling is being performed to extract the image features when applying the *DFT* and this method is more robust to small angle rotations. Lei *et al*. [46] first proposed a *RT* and then computed its moment features before applying *DFT* of every moment. The first fifteen significant *DFT* from the starting coefficients were then normalized and quantized according to their requirements to obtain the image hash value. This scheme shows satisfactory results when it is facing geometrical distortions in image pixels.

Matrix decomposition based image hashing methods:- Various methods are based on matrix decomposition. Kozat et al. [27] based on singular value decomposition (*SVD*) to get robust image features from the image and also to generate an image hash matrix. This hashing algorithm mainly consists of two major steps. In the first step, intermediate features are extracted using pseudo random (*PR*) and semi global regions via *SVD*. In the second step, the *SVD* which is obtaining from first step is again applied to the intermediate features to construct the final hash matrix. Monga *et al.* [41] also proposed a new method based on *PR* signal representation method using non-negative matrix factorization (*NMF*) for extract the features and to construct the image hash. This function shows better performance as compared to the *SVD* based method. Recently, Tang et al. [57] introduce a robust image hashing function which is basically based on ring partition and *NMF* and the results show good performance of common content preserving operations and large angle rotation operation in image hash.

Others image hashing methods:- Xiang *et al.* [64] introduce a histogram based image hashing method, which is robust to geometric distortions of image pixels but not to additive noise, brightness adjustment and contrast enhancement in image pixels. Battiato *et al*. [7] introduce an image representation based on a set of *SIFT* features and it is known as bag of features (*BOF*) to construct the hash matrix and explored a non uniform quantization of histograms oriented gradients (*HOG*) in image pixels and to get tamper localization capabilities. Zhao *et al*. [69] construct an image hash by combining global

and local features of image hash. The global features of image are corresponding to the Zernike moments of the luminance and chrominance components, while the local features of image are include both the positions and the texture information of salient regions in hash. This function can identify the image tamper as well as the modified locations of an image. Other methods for feature extraction are constructing image hashes also reported including the random Gabor filtering [35] and the ring partition [56] and shape contexts [38].

When we applied these methods to color images, most of the above techniques convert three color channels *i.e.* Red, Green and Blue into gray scale images while discarding the information of chrominance from an image. While discarding the information of chrominance may not only improve the detection performance in images [44, 69], but may also make image tempering more difficult due to the fact that the hash matrix contains both luminance and chrominance factor. *DWT* simultaneously deal with the three color channels without discarding the chrominance information and they have already been successfully implemented in color image registration [59], image analysis [17, 18, 26, 43, 47] and watermarking [10, 28, 58]. Recently, *DWT* was used to generate image hashing and applied to image retrieval [29].

Chapter 3: A Multilevel Hybrid Chaotic Cryptosystem for Digital Images

3.1. Introduction

Today, important information send over internet is not only text data, but also contain multimedia information like image, video and audio data *etc*. Some conventional cryptographic systems directly convert image data into encrypted form of data. But this is not advisable due to very huge data size of image data and a real-time constraints of such type of data. Conventional cryptosystem require huge amount of time to direct convert thousands of image pixel values into encrypted form and in image data, a decrypted image is normally acceptable even if it contain small level of distortion in image data [50]. For all these reasons, the methods that perform well for text data may not be suitable for image data.

In this Chapter, a multilevel hybrid chaotic cryptographic system for digital images is proposed. It is basically combination of public and private keys or hybrid technique to encrypt the image. Plain and secret images are encrypted using *RSA* algorithm using p and q rounds of execution respectively. Cipher images are generated using *XOR* operations on encrypted plain and secret images. To show the effectiveness of the proposed system, *NPCR* and *UACI* metric have been calculated for five text images for five rounds. In each round, public key encryption is applied in the form of *RSA*. Due to some iteration applied on the chaotic system to obtain the cipher-image the security level will increase.

3.2. Problem Statement

The two main problems that arise in image encryption process are with respect to time it takes for its computation and its security level. For real time image encryption only those ciphers are preferable which takes lesser computation time without compromising security. An encryption scheme which runs very slow, even through may have higher

degree of security features would be of little practical use for real time processes. Hence a trade off has to be made.

Many encryption methods have been proposed in literature, and the most common way to protect large multimedia data is by using conventional encryption technique. Private Key bulk encryption technique such as DES and AES, are not suitable for transmission of large data. Due to the complexity of their internal structure, image encryption algorithm can become an integral part of the image delivery process if they aim towards efficiency and at the same time preserve the security level.

3.3. Proposed Work

Proposed cryptosystem for digital images is explained in this section. This system contains two processes: encryption and decryption which are depicted in Figure 3.1 and 3.2 respectively.

3.3.1. Encryption Process

Figure 3.1 presents the architecture of the proposed encryption scheme. This scheme has two input, two main functions and the final result *i.e.* the encrypted image. The plain image, secret image are the two main inputs for this model. The primary functions are *RSA* encryption and pixel modification.

As illustrated in Figure 3.1 at the first step, *RSA* encryption is applied on plain image as well as secret image for p and q rounds respectively to get encrypted image. The outputs of these two phases are applied to pixel modification, which is a sequence *XOR* of consecutive pixels of the encrypted original image and the encrypted secret image. The result is fed back to the *RSA* Encryption function and this process runs for r rounds. After r rounds the output of the pixel modification function is the cipher image.

3.3.1.1. RSA Encryption

Encryption is a process to transform readable type of information into a form that was unreadable by any user. *RSA* is the best widely used asymmetric-key type of data encryption in cryptography [45]. *RSA* encryption process include following steps:

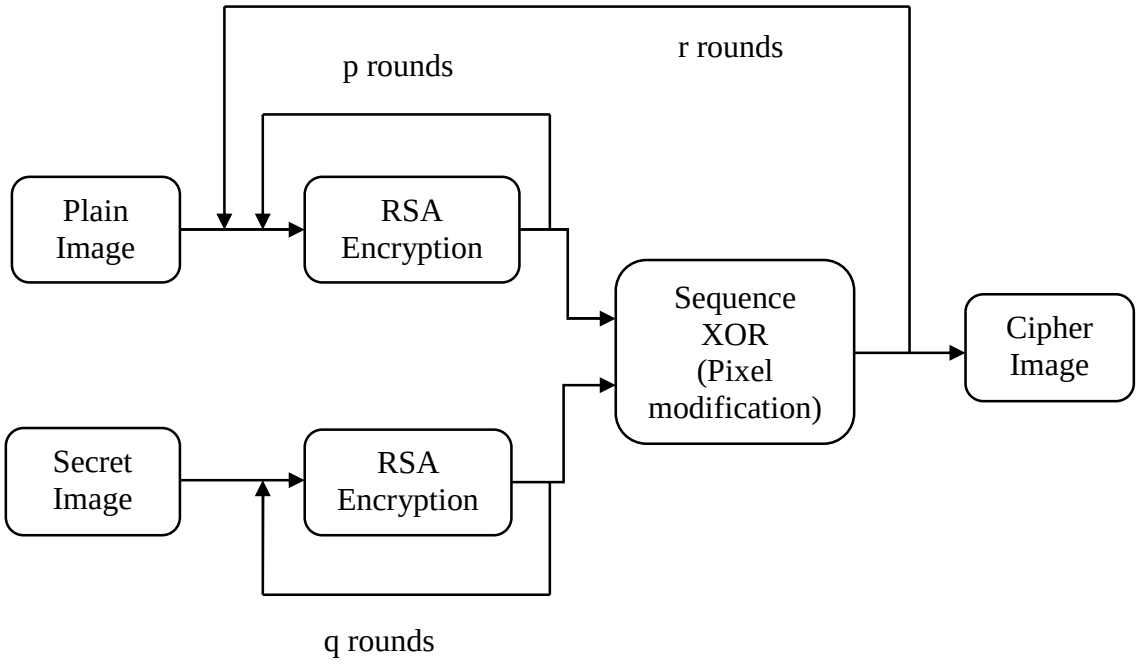


Figure 3.1: Encryption Process used in Proposed Scheme

i. In this each user sender and receiver both calculating the public and private key pairs for transferring data.
ii. For key pairs they have to select 2 prime numbers that should be large *i.e. a* and *b*.
iii. Now, compute the modulo by computing *R* and $\phi(R)$ such that $R = a \times b$ and $\phi(R) = (a-1)(b-1)$.
iv. Now, randomly choose the encryption key *k* so that, $\gcd\big(k, \phi(R)\big) = 1$, where $1 < k < \phi(R)$
v. Also compute the decryption key *k1* so that $k \times k1 = 1 \bmod \phi(R)$, where $0 \leq k1 \leq R$
vi. Now, publish both public and private key.
vii. To encrypt the message *M* into cipher text *C* use formula $C = M^e \bmod N$, where $0 \leq M < N$.
viii. And to decrypt the plain text from cipher text use formula $M = C^d \bmod N$.

3.3.1.2. Pixel Modification

In this phase, pixels are changed with respect to secret image. The *XOR* operation is applied on encrypted image with secret encrypted image. So the extreme change occurs

in the cipher image pixels. The output of this function is modified image and this step is repeated for *r* rounds for cipher image.

3.3.2. Decryption Process

Figure 3.2 shows the decryption process in which the plain image is recreated using the secret image. Inverse pixel modification is performed on the cipher image and the secret image after $q \times r$ rounds of *RSA* encryption. The result of the secret image *RSA* encryption in the first step is saved for subsequent steps of *RSA* decryption function. Now this applies for *r-1* rounds for *RSA* decryption and this image and cipher image is applied as an input to the inverse pixel modification function.

The additional input is (the feedback of) the output of the inverse pixel modification function after *r-1* rounds of *RSA* decryption.

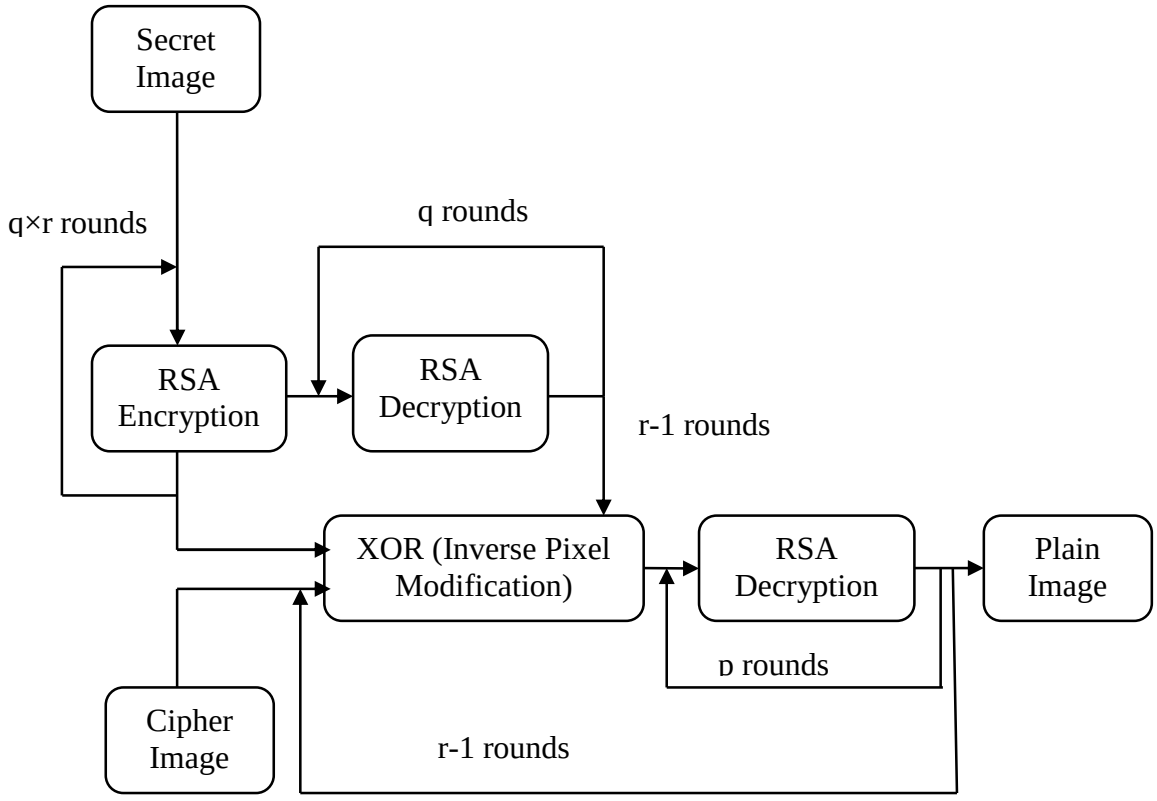


Figure 3.2: Decryption process used in Proposed System

3.4. Experimental Results and Analysis

Experiments are carried out to check the randomness and security of cipher or encrypted image. Various experiments are carried out like key sensitivity analysis, key space analysis and differential analysis etc. are carried out to prove the effectiveness and efficiency of the algorithm.

3.4.1. Key Space Analysis

In the key space analysis shows that the number of possible combination of keys from which attacker can try to break a cryptosystem. The total numbers of different combination must be significantly more to protect brute force attack from attackers. In the developed system, the secret image was used as the initial secret key and the different prime numbers are used for different rounds of iterations are the other secret keys for this cryptosystem. Some other control parameters for particular cryptosystem are *p*, *q* and *r* rounds. These parameters are number of iteration for different rounds for different functions. The parameter *p* is controlling the number of rounds for encryption of plain image, *q* is controlling the number of rounds for secret image or key image and *r* is used to control the number of rounds for final iteration of the loop. The final loop is used to improve the security and randomness of the proposed system. These parameters should be kept secret because they are used as the secret keys. In proposed work the combination of these parameters will provide a large key space of approximately 2^{250} that is sufficient to make brute force attack infeasible. This combination is very large as compared to previous works.

3.4.2. Key Sensitivity Analysis

In addition to a sufficiently huge key space in the key analysis for preventing a encrypted image from brute force attacks from attackers, a strength algorithm should also be applied and that is sensitive to with encryption and decryption keys. Sensitivity means changing even one bit in a secret key image will outcomes a completely different image as a result in both encrypted image and the decrypted image. In both the encryption and the decryption phase the key sensitivity is analyzed. In the encryption phase, the different

cipher image is obtained by just changing one bit in a secret image and in any key which is used in encryption phase. In the decryption phase, the key sensitivity analysis will show that the decrypted images are different when we use the different parameters at the decryption time. Based on this fact changing even single bit in the encryption key will produce different plain image as a result. The difference rates of two encrypted images and the decrypted images are shown in Table 3.1 and Table 3.2 respectively.

Table 3.1: Difference rates of two encrypted images with slight change in a parameter

Parameter	Initial value	Changed value	Encrypted image change rate
p	1	2	94.72%
q	1	2	96.03%
r	1	2	95.32%
a	11	13	94.67%
b	31	29	96.64%

Table 3.2: Difference rates of two decrypted images with slight change in a parameter

Parameter	Encryption parameter	Decryption parameter	Decrypted image difference rate
p	2	1	96.97%
q	2	1	96.02%
r	2	1	95.87%
a	11	13	96.76%
b	31	29	95.11%

3.4.3. Statistical Analysis

Statistical analysis is represents the relationships of the original image and the encrypted one. In Shannon's theory it is proved that it is possible to break many types of cryptograms by using the statistical analysis [50]. This can be achieved by reducing the redundancy in the structure of the message by applying diffusion or by increasing the complexity of the relationship between the cipher image and the secret key image by confusion and diffusion. One of the factors from either confusion or diffusion is present in the proposed cryptosystem to frustrate statistical attacks from the attackers.

3.4.3.1. Entropy Analysis

Entropy is one of the statistical parameter that is used to measure the uncertainly and randomness of a large image data. According to theory of Shannon for cryptography, image entropy is defined as the number of bits that is necessary to encode every pixel of the image data. The entropy shows the random pattern of image data and texture of pixels in a cipher image. The entropy values of original images and the encrypted images given in Table 3.3.

Table 3.3: Results of entropy of plain and cipher image

Image name	p	q	r	Plain entropy	Cipher entropy
Baboon	1	1	1	7.6031	6.4002
	3	1	1		3.1884
	1	3	1		4.2361
	1	1	3		2.9175
Hydrangeas	1	1	1	7.1026	6.1903
	3	1	1		3.3747
	1	3	1		4.1277
	1	1	3		2.8562
Desert	1	1	1	7.6747	7.3566
	3	1	1		5.3025
	1	3	1		4.255
	1	1	3		2.8921
Lighthouse	1	1	1	7.3991	6.4887
	3	1	1		3.3907
	1	3	1		4.2818
	1	1	3		2.8175
Parrot	1	1	1	1.9734	4.7557
	3	1	1		4.1033
	1	3	1		2.8833
	1	1	3		2.4401

3.4.4. Differential Analysis

For differential type of attack, an attacker try to trace difference between two images one is encrypted image and another is image that is obtain by changing a specific pixel in the plain image to find a meaningful relation between them and this is also known as a

chosen plaintext attack. An encrypted image is very sensitive to minor changes and even changing single bit in the original image will result in very different encrypted image.
NPCR factor measures the number of pixels change rate in the encrypted image with only 1 bit is changed in the plain image. This parameter is calculated by (3.1) and for an ideal encryption algorithm it is considered as 1.

$$\text{NPCR} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} f(i,j) \times 100$$

$$\text{f(i, j)} = \begin{cases} 0 & if\ e1\ (i,j) = e2\ (i,j), \\ 1 & if\ e1\ (i,j)\ \neq e2\ (i,j), \end{cases} \quad (3.1)$$

Where, e*1* and e*2* are obtained by encrypting different $m \times n$ plain image and having only one random bit dissimilarity, means changing one bit while encrypting the image.
Another differential analysis parameter is *UACI* (Unified Average Changing Intensity) between two encrypted images with a difference in only one bit in corresponding plain images. The *UACI* can be calculated by (3.2):

$$\text{UACI} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{|\, e1\ (i,j) - e2\ (i,j)|}{2} \times 100 \quad (3.2)$$

To evaluate the sensitivity a random bit is changed in the plain image of the proposed cryptosystem to differential attacks. Encrypting two plain images for obtaining two cipher images with a difference in only one bit change in the image. The rates of change pixel and intensity differences in the two encrypted images are calculated and the results are shown in the following tables.

Table 3.4: Calculated *NPCR* and *UACI* for different combination of *p*, *q* while *r*=1 in Desert image

p/q		1	2	3	4	5
1	NPCR	98.2508	98.9193	91.1412	88.0005	88.4559
	UACI	17.5031	16.4466	11.6851	9.6583	10.5674
2	NPCR	98.0633	97.9741	92.1574	88.0197	88.0775

	UACI	14.4693	15.2105	12.1399	9.6357	9.9477
3	NPCR	88.5881	89.1219	91.4634	88.874	86.7985
	UACI	8.2983	9.293	11.9285	10.0931	8.5877
4	NPCR	84.9032	85.7608	83.7878	87.291	85.2304
	UACI	6.0641	6.9519	6.3575	8.669	7.3379
5	NPCR	82.1948	84.6128	83.2498	85.4307	83.7164
	UACI	3.4571	4.6912	5.8123	4.2907	4.9341

Table 3.5: Calculated *NPCR* and *UACI* for different combination of *q*, *r* while *p*=1 in Desert image

r/q		1	2	3	4	5
1	NPCR	98.2508	99.1853	91.1693	92.5454	91.8814
	UACI	17.5031	17.2091	11.7348	9.6553	7.9273
2	NPCR	98.0633	98.6812	94.6842	92.1574	88.0197
	UACI	14.4693	15.3641	12.6789	12.1399	9.6357
3	NPCR	88.5881	95.3874	93.9438	91.4634	88.874
	UACI	8.2983	13.2571	11.9435	11.9285	10.0931
4	NPCR	84.9032	89.3974	90.9124	83.7878	87.291
	UACI	6.0641	9.7812	9.2764	6.3575	8.669
5	NPCR	82.1948	87.5412	88.6183	83.2498	85.4307
	UACI	3.4571	6.3812	7.9106	5.8123	4.2907

Table 3.6: Calculated *NPCR* and *UACI* for different combination of *p*, *r* while *q*=1 in Desert image

p/r		1	2	3	4	5
1	NPCR	98.2508	98.9193	91.1412	88.0005	88.4559
	UACI	17.5031	16.4466	11.6851	9.6583	10.5674
2	NPCR	99.1853	97.9741	94.6842	92.1574	88.0775
	UACI	17.2091	15.2105	12.6789	12.1399	9.9477
3	NPCR	91.1693	95.5403	90.7103	91.4634	85.7608
	UACI	11.7348	12.9204	10.6401	11.9285	6.9519
4	NPCR	92.5454	93.4237	88.3429	89.3974	84.9032
	UACI	9.6553	10.4031	8.0347	9.7812	6.0641
5	NPCR	91.8814	91.3019	83.2498	86.7985	83.7878
	UACI	7.9273	8.4278	6.3575	8.5877	6.3575

Table 3.7: Calculated *NPCR* and *UACI* for different combination of *p*, *r* while *q*=1 in Baboon image

p/r		1	2	3	4	5
1	NPCR	99.5286	99.6342	92.4681	86.5755	89.2442
	UACI	16.7966	16.6342	12.6423	8.871	10.0601
2	NPCR	99.5949	88.9269	88.5413	85.762	87.6197
	UACI	16.8425	9.844	10.9587	8.0871	9.3348
3	NPCR	91.8022	87.8103	82.788	88.5729	86.9173
	UACI	11.5174	7.739	5.3687	8.719	8.6271
4	NPCR	86.7622	85.9073	84.3184	85.9137	84.2904
	UACI	8.5517	6.0197	6.8246	7.1764	6.2791
5	NPCR	85.9508	82.6371	82.4961	84.4961	82.6719
	UACI	8.4953	5.9173	6.7037	5.2384	6.8237

Table 3.8: Calculated *NPCR* and *UACI* for different combination of *p*, *r* while *q*=1 in Hydrangeas image

p/r		1	2	3	4	5
1	NPCR	99.4372	98.3361	99.5195	99.1698	99.4672
	UACI	17.5486	13.6517	26.1256	18.3481	17.3809
2	NPCR	99.8711	88.9484	83.4093	82.8409	79.6847
	UACI	17.2741	10.8386	5.5717	4.9079	3.9991
3	NPCR	94.3851	90.5712	85.6137	84.361	80.9105
	UACI	14.6471	12.3691	10.5713	7.9108	6.0224
4	NPCR	89.1698	87.1907	83.273	82.3709	79.3007
	UACI	9.7871	9.6107	7.2491	6.8107	5.3371
5	NPCR	88.6472	85.0152	82.2018	80.9411	78.2897
	UACI	10.2792	8.0483	5.7035	5.3104	5.3077

Table 3.9: Calculated *NPCR* and *UACI* for different combination of *p*, *r* while *q*=1 in Lighthouse image

p/r		1	2	3	4	5
1	NPCR	99.3512	98.4821	98.4032	99.709	98.2473
	UACI	17.9138	14.2019	25.6971	18.349	16.8205
2	NPCR	99.3482	94.9372	94.2791	93.4673	94.2189
	UACI	16.9147	10.8386	14.0541	13.4672	12.356
3	NPCR	95.3746	92.8103	91.9108	91.0197	92.7913
	UACI	15.9438	11.3795	11.3719	10.3195	10.491
4	NPCR	92.9716	91.3746	88.0064	90.8216	88.4612

	UACI	10.8437	11.8469	10.4963	10.9726	9.7613
5	NPCR	90.9643	88.9432	85.1149	88.3496	85.4692
	UACI	11.9137	9.3718	9.8874	9.2179	7.0237

Table 3.10: Calculated *NPCR* and *UACI* for different combination of *p*, *r* while *q*=1 in parrot image

p/r		1	2	3	4	5
1	NPCR	98.2508	98.4821	98.4032	99.1698	99.4672
	UACI	17.5031	14.2019	25.6971	18.3481	17.3809
2	NPCR	99.1853	94.9372	94.2791	82.8409	79.6847
	UACI	17.2091	10.8386	14.0541	4.9079	3.9991
3	NPCR	91.1693	90.5712	82.788	84.361	85.7608
	UACI	15.9438	12.3691	5.3687	7.9108	6.9519
4	NPCR	92.9716	87.1907	84.3184	85.9137	84.9032
	UACI	10.8437	9.6107	6.8246	7.1764	6.0641
5	NPCR	90.9643	88.9432	82.4961	84.4961	83.7878
	UACI	11.9137	9.3718	6.7037	5.2384	6.3575

The above tables are shows the randomness of the pixels in the encrypted images and the *NPCR* and *UACI* will show the effectiveness of the algorithm. The results will show that as the value of *p* will increase the randomness of the image pixels will also increase.

3.5. Conclusion

In this Chapter, a cryptographic system for digital images is proposed. Proposed system is multilevel and chaotic in nature. Plain and secret images are encrypted using *RSA* algorithm using *p* and *q* rounds of execution respectively. Cipher images are generated using *XOR* operations on encrypted plain and secret images. To show the effectiveness of the proposed system, *NPCR* and *UACI* metric have been calculated for five text images for five rounds of different combinations of *p*, *q* and *r*.

Chapter 4: Hashing based Image Authentication using Multiple Transforms

4.1. Introduction

In this Chapter, Image hashing scheme for image authentication is proposed based on the multiple transformations *i.e. DWT* with the log-polar transform. *DWT* jointly deal with all the three combination of color in an image and also it uses very less computation time with respect to other transformations. The main features of the proposed method are based on (i) the secondary image is obtained by log polar transform and (ii) the addition of images that are formed by log polar transform with the output of the *DWT* applied on the image after pre-processing. The final hash image is generated by applying the Arnold transformation on the result image according to the correlation of these magnitude coefficients and is scrambled by a secret key to enhance the system security. Various results are obtained by conducting some experiments in order to analyze and identify the most appropriate parameter values of method that has been proposed and results will also show the quality of image not much distracted in proposed method. This scheme also shows the better sensitivity when changing the little part of image.

By following the same path, we proposed an Arnold image hashing method based on *DWT* and log-polar transform for image authentication. *DWT* handle simultaneously all the three channels *i.e. RGB* of color image without discarding chrominance and luminance information. Similar to *DWT*, the low frequency coefficients of *DWT* contain the important part of energy of the image and represent essential image features. In addition to *DWT* combined with the log-polar transform so that it can achieve a set of most essential features that are rotation invariant of an image. We propose a method to take advantage of *DWT* used it to build an Arnold and hash image that is robust to content preserving operations, geometric attacks while being sensitive to various malicious tampering attacks.

4.2. Proposed Scheme

This robust image hashing technique is shown in Figure 4.1. In this robust hashing scheme, it includes 3 steps *i.e.* first step is image pre-processing stage followed by an image feature extraction process and last step is hash construction.

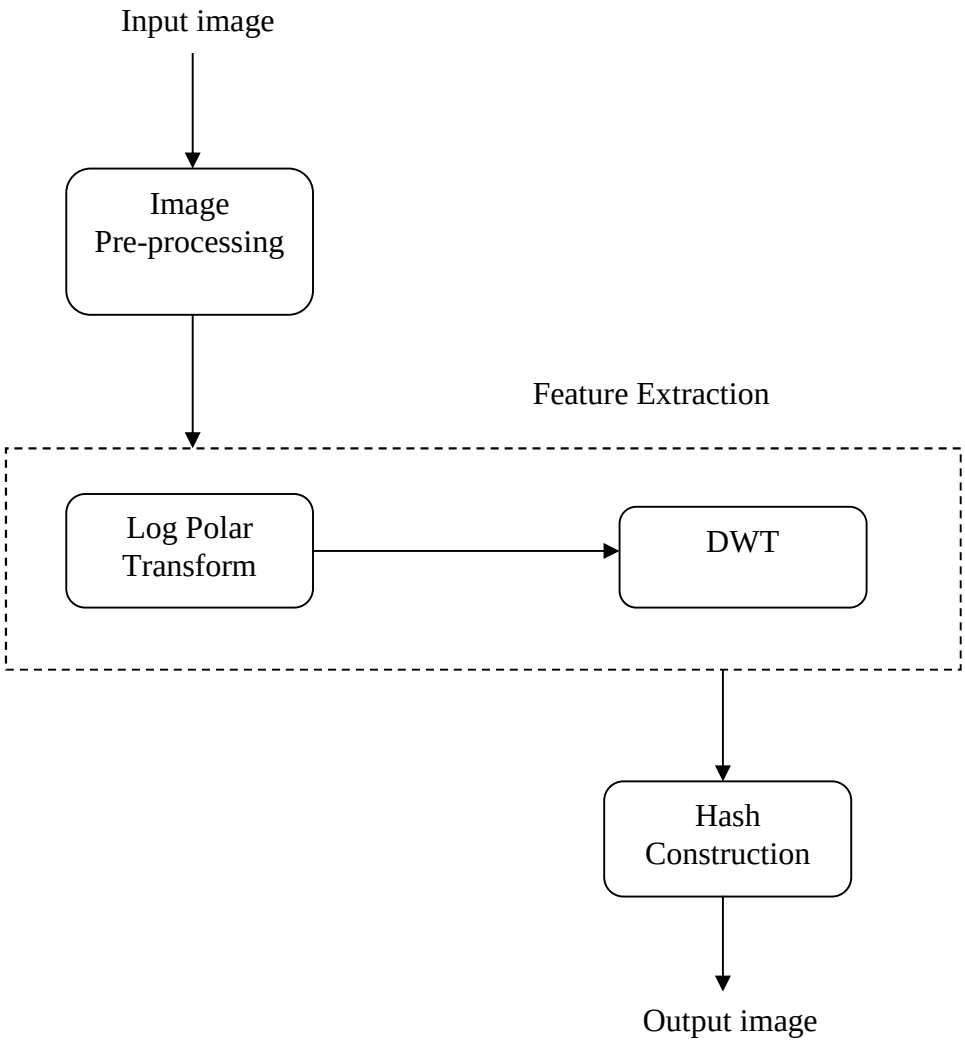


Figure 4.1: Block diagram of Arnold image hashing scheme

4.2.1. Pre-processing

The pre-processing step of proposed scheme is shown in Figure 4.2 for Lena test image. This scheme will take I_0 image as an input and this is first rescaled to a fixed size $M \times M$

image. This step of proposed scheme will ensure that the generated image matrix will be of fixed size while making it robust against applying image scaling operation on fixed size image and image matrix. In the proposed work, size of matrix of image 256×256 chosen. In the second step of image pre-processing, to make the generated image hash is more robust, an averaging filters or smoothing filter will be applied based on a $k\times k$ window size. Its main aim is to preserve or extract the essential features of structures while removing insignificant details without disturbing the image content.

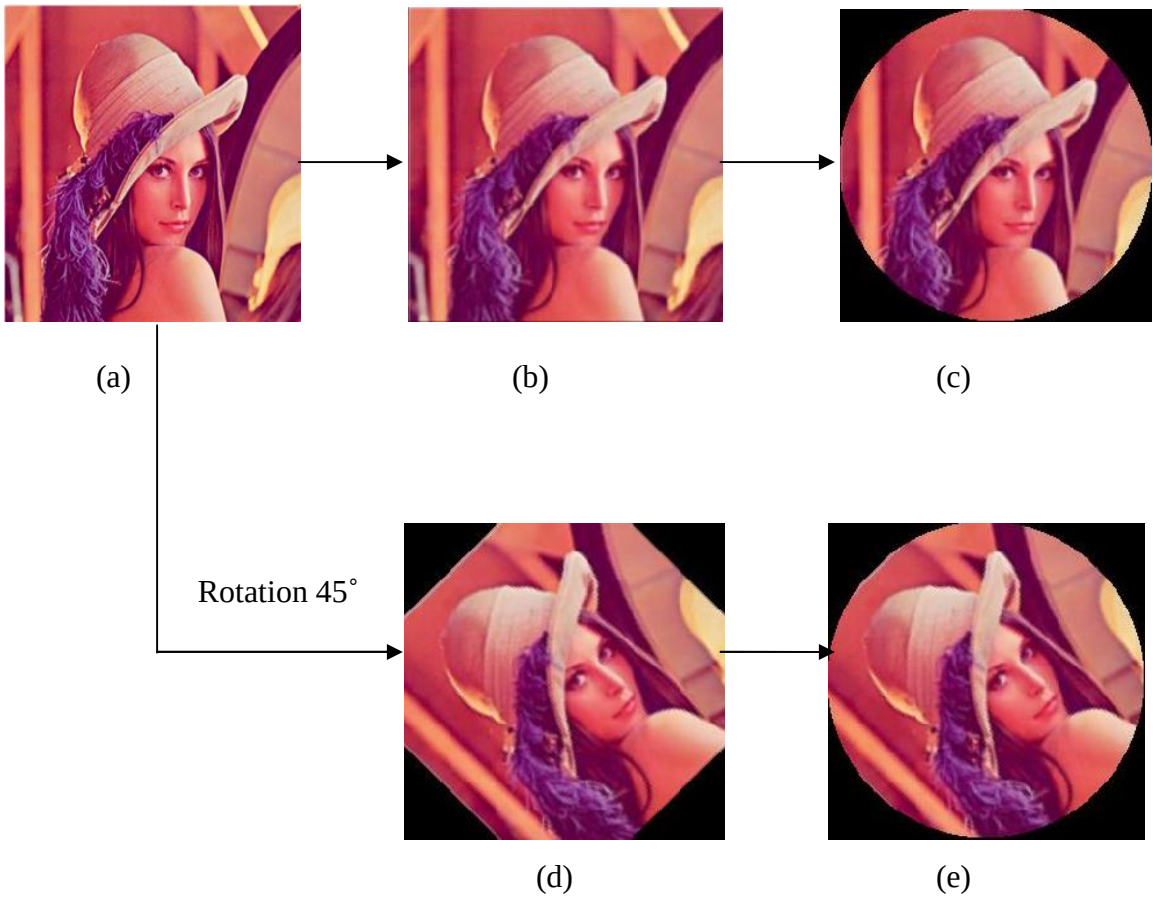


Figure 4.2: Pre-processing procedure applied to lena image and its rotated version of an angle of 45 degree. (a) Image I_0, (b) and (c) Smoothed images of lena image, (d) and (e) inscribed circle in smoothed images of (b) and (c).

The next step is to rotate an image according to requirements of the proposed scheme and we propose to only consider the pixels that are inside the image circle as illustrated in

Figure 4.2 (d). This step is performed by setting to zero all the pixels that are outside the inscribed circle. As shown in Figure 4.2 (d) and Figure 4.2 (e), the same pixel values of the image and its rotated version. This will allow us to minimize the influence of information loss, especially the loss of pixels due to the image corner. In the case of image rotations we will use 45 degree of large angle rotation.

4.2.2. Feature Extraction

In the pre-processing step the robustness of image scaling being handled, the image features that we are looking for should be robust for image rotation and for that, we apply log-polar transform as the first transform in the pre-processing stage on to the image and then to apply the *DWT* on the output of the particular image.

Let $f_1(x, y)$ is a function of a rotated version of the original color image i.e. $f_0(x, y)$ with rotation angle is θ_0:

$$f_1(x, y) = f_0 [(x\cos\theta_0 - y\sin\theta_0), (x\sin\theta_0 + y\cos\theta_0)]. \quad (4.1)$$

If we are using the log-polar coordinates as:

$$x = e^{\rho} \cos\theta, \text{ and}$$

$$y = e^{\rho} \sin\theta, \quad (4.2)$$

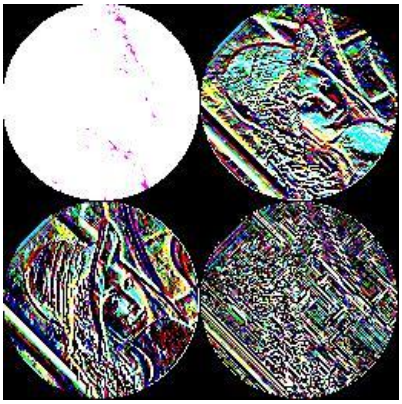
where $\rho = \ln[(x-x_0)^2+(y-y_0)^2]^{1/2}$ represents the log value of the radial distance from the origin (x_0, y_0) of the image pixels, $\theta = \arctan((y-y_0)/(x-x_0))$ is represents the polar angle in the log-polar system, e is the base of the log in the log-polar system, the origin (x_0, y_0) being located at the center in log-polar system of the image. So the, Eq. (4.1) can be rewritten as [59]:

$$f_1(\rho, \theta) = f_0[\rho, (\theta+\theta_0)]. \quad (4.3)$$

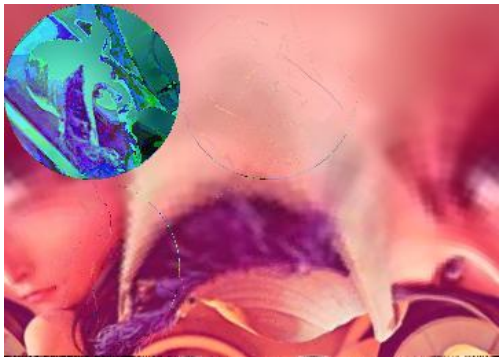
Eq. (4.3) represents the cyclical shift θ_0 along the angle axis in the image rotation. The results that will come out from the log-polar transform when we will apply to the pre-processed images given in Figure 4.2 (e) is shown in figure 4.3 (a). As it seen in the results of the images, they are very much similar except for a cyclical translation along

the horizontal axis in the images. Now on Eq. (4.3) we are applying the *DWT* by which the frequency coefficients of the image are translated in very short time period and it will shown in figure 4.3 (b). Due to the fact that the low-frequency components of *DWT* hold the major part of the image pixel energy and represent the main information on the image content, like for the *DFT*, we propose this method to use the magnitude of these low-frequency coefficients of image pixels as features.

(a)



(b)



(c)

Figure 4.3: Results of feature extraction step. (a) Results of log-polar transform when it is applied on image shown in Figure 4.2 (e), (b) result of *DWT* when it is applied on output of the log-polar transform and (c) result of *XOR* of both the images.

If the feature extraction part of a hashing matrix technique is not dependent on the knowledge of a secret key and if it is not secured using the key than it is not possible to reconstruct the image that are completely different from the previous one or we able to destroy the hash by introducing small distortion into the image pixels [60]. In order to secure hash matrix of the image, we apply the Arnold transform [5, 10], because it is parameterized by using the secret key *K*, so as to secretly scrambled the *DWT* coefficients.

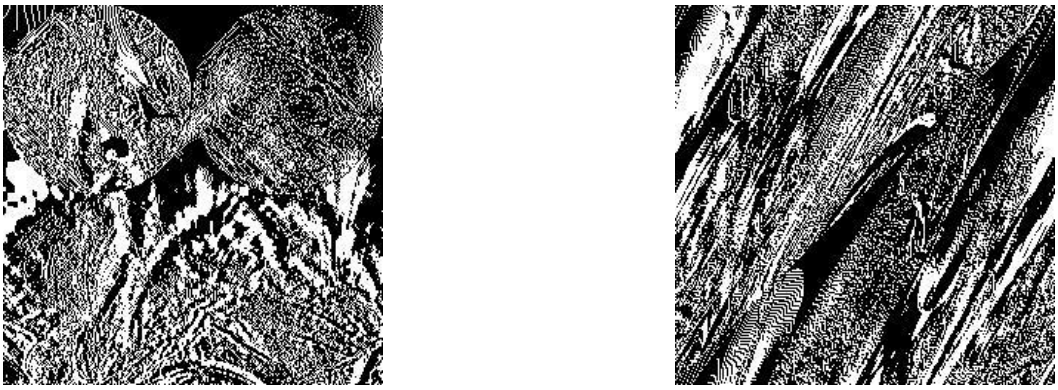
To *XOR* the both *DWT* and log-polar transform and the output from that are used in our scheme to capture image features and from which our image hash is built and it will shown in Figure 4.3 (C).

4.2.3. Hash Construction

Let us represent the magnitude coefficients of the resulted image that will come out from XOR operation of the log-polar transform and the *DWT* transform into a row vector X=[x(1), x(2), ..., x(p)], where x(i) corresponds to the i^{th} magnitude coefficient of vector X, and i = 1, ..., p. Each x(i) is determined from the square region of the image according to the selection of sequence from top to bottom and from left to right in image pixel matrix. The robust hash matrix H_G is generated using the following formula [61]:

$$H_G(i) = \begin{cases} 1, & \text{if } x(i) - x(i+1) \geq 0, \\ 0, & \text{if } x(i) - x(i+1) < 0, \end{cases} \qquad i = 1,..., p-1. \quad (4.4)$$

For the purpose of increasing the security and the quality of H_G matrix the H_G matrix is secretly scrambled based on a permutation process by using a secret key K_H. For this purpose we use the Arnold transformation and by using this transformation we generate a new hash matrix H_{G0} with correspondence to the H_G hash matrix and they are show in Figure 4.4. According to the secret key it will generate the new matrix and that matrix cannot be constructing without using the secret key. This new hash matrix H_{G0} is used to authenticate the original image by sending it with the original image.



(a) (b)

Figure 4.4: Results of hash construction phase. (a) Initial hash matrix $H_{G,}$ (b) Final hash matrix H_{G0}

4.2.4. Image Authentication

In a traditional scenario, the robust hash matrix H_{G0} is transmitted along with the original image I_0 through the Internet or a third party certification organization. At the receiver end the recipient can check the image authenticity by applying the same procedure to the received image. Suppose the received image is I_1 that is a version of I_0 that may have undergone some malicious tampering operations and some content preserving operations and it is utilized to generate the hash matrix H_{G1} according to the same procedure that is used to generate the H_{G0} matrix. Now these two hash matrix H_{G0} and H_{G1} are compared to determine whether the received image is changed or not. If the two hash matrix H_{G0} and H_{G1} are same then the received image is same as the transmitted image otherwise the original image is tempered and the received image is changed.

4.3. Experimental Results

4.3.1. Image Data Sets

To analyze the results of the developed technique the image database are used which including some color images of size 256×256 pixels was selected. In the proposed scheme we are using some images that are shown in Figure 4.5 and all the experiments are performed on these images.

The various parameters evaluate to show the authentication performance in proposed scheme. They are defined as follows:

4.3.2. Performance Analysis

In order to better evaluate the performance of our proposed scheme some parameters are to be measured these parameters are *PSNR, NPCR* and *UACI. PSNR* ratio shows the quality of image after constructing hash matrix and it will show in Table 4.1.

The *NPCR* measures the number of pixels change rate in hash matrix when only 1 bit is changed in the original image. This parameter is calculated by (4.5) and for an ideal algorithm it is consider near about 1.

$$\text{NPCR} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} f(i,j) \times 100$$

$$\text{f(i,j)} = \begin{cases} 0 & if\ e1\ (i,j) = e2\ (i,j), \\ 1 & if\ e1\ (i,j) \neq e2\ (i,j), \end{cases} \tag{4.5}$$

Where, *e1* and *e2* are obtained by hash matrix of two $m \times n$ plain images and any bit dissimilarity.

The *UACI* in differential analysis is the unified average changing intensity between two hash matrixes with a difference in only one bit in corresponding original images. The *UACI* can be calculated by (4.6):

$$\text{UACI} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{|e1\ (i,j) - e2\ (i,j)|}{2} \times 100 \tag{4.6}$$

To evaluate the sensitivity of the proposed algorithm to differential attacks, we changing a random bit in the original image. Hash matrix of two plain images with a difference in only one bit produces two new hash matrixes. The rates of pixel and intensity differences in the two hash matrix are calculated. The results are shown in the Table 4.2.

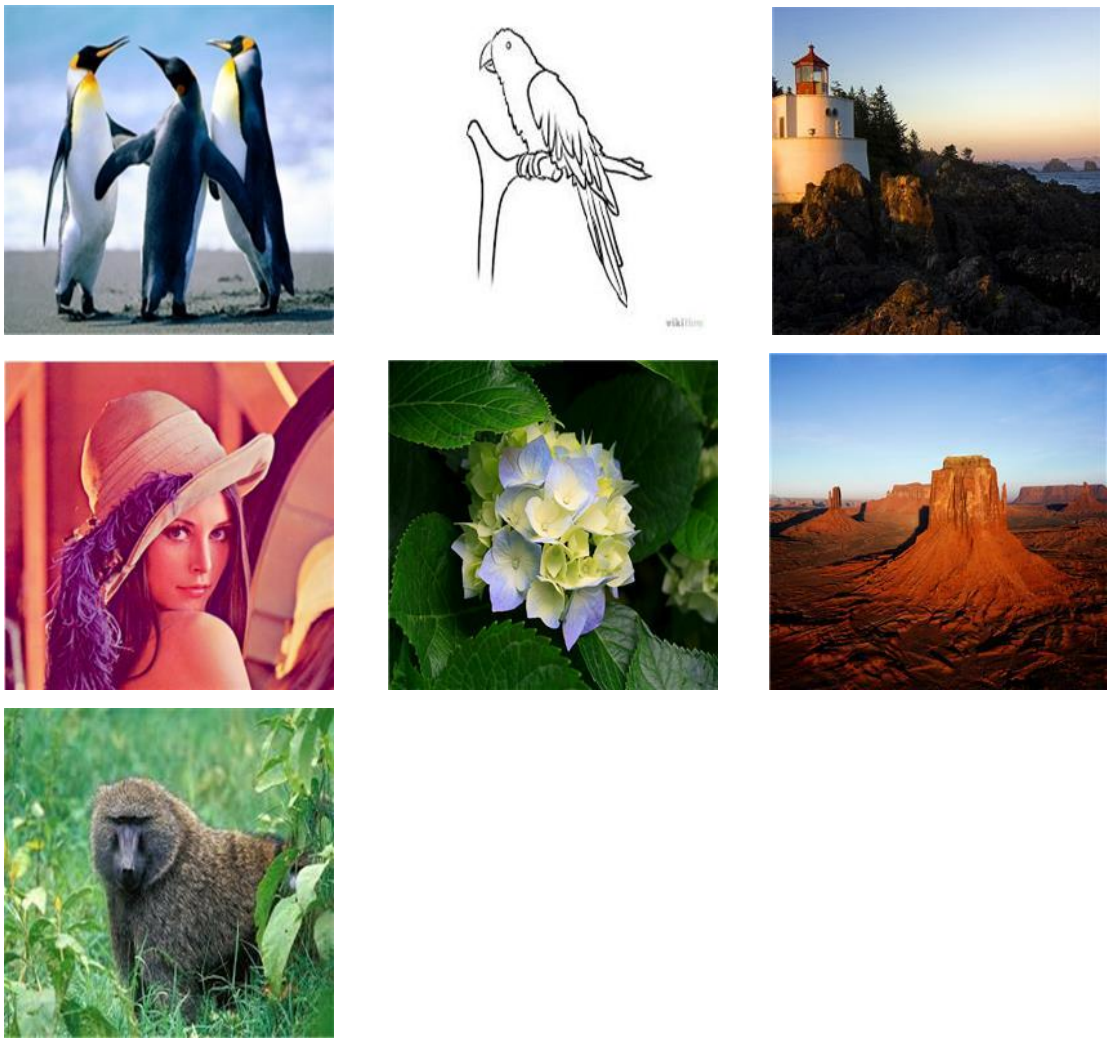


Figure 4.5: Examples of test images.

Table 4.1: Result of *PSNR* for different images

Image	**MSE**	**PSNR**
Baboon	106.05	27.91
Parrot	4.56	41.57
Desert	83.78	28.94
Hydrangeas	94.06	28.43
Lighthouse	79.42	29.17
Penguins	72.16	29.58
Lena	96.6	28.32

Table 4.2: Results of *NPCR* and *UACI* for different images

Image	NPCR	UACI
Baboon	83.0384	44.3481
Parrot	70.5841	33.6431
Desert	80.1572	35.7159
Hydrangeas	77.9588	35.2416
Lighthouse	78.0693	32.0852
Penguins	78.6022	33.4589
Lena	81.6994	41.3028

4.3.3. Sensitivity Analysis

In addition to a sufficiently large key space in key analysis to protect a hash matrix from brute force attacks from attackers, a strength algorithm should also be applied and that is very much sensitive to with keys. Sensitivity means changing even one bit in a hash matrix will outcomes a completely different hash matrix as a result in proposed scheme. In our proposed scheme we analyzed this by changing only the 1 column of hash matrix. In first case we take hash matrix from the first column and in second case we take it from the 2^{nd} column and the result will show the completely different hash matrix and it will show in Table 4.3.

Table 4.3: Difference rates of two hash matrix with slight change in a parameter

Image	Parameter	Initial value	Changed value	Encrypted image change rate
Baboon	HG1 square matrix	from 1st column	from 2nd column	82.44%
Parrot	HG1 square matrix	from 1st column	from 2nd column	78.36%
Desert	HG1 square matrix	from 1st column	from 2nd column	78.63%
Hydrangeas	HG1 square matrix	from 1st column	from 2nd column	80.81%
Lighthouse	HG1 square matrix	from 1st column	from 2nd column	78.74%
Penguins	HG1 square matrix	from 1st column	from 2nd column	77.43%
Lena	HG1 square matrix	from 1st column	from 2nd column	80.67%

4.4. Conclusion

In this Chapter, we proposed a hashing based image authentication algorithm for color images using *DWT* and log-polar transforms. By XORing the *DWT* with the log-polar transform, we better take account into the three image color planes and the resulting hash is more robust to rotation attacks from the attackers and also to common image content preserving operations. The various parameters have been determined to check the quality of algorithm by means of intensive experiments on a large image data set so as to establish good tradeoffs in content preserving operations in terms of hash robustness against average filtering and large angle rotation attacks. And also show the good sensitivity to the unauthorized image content alterations by changing the position of hash matrix by just 1 column. Compared to the other hashing technique our scheme provides the overall a better performance. As the future work we will focus on designing a new robust hashing scheme that can capable to locate tampered regions using the hash matrix of an image as well as to determine the type of the tampering in the image.

Chapter 5: Conclusion and Future Work

In this thesis, a cryptographic system for digital images and an Arnold robust image hashing algorithm is proposed. In chaotic cryptosystem the plain and secret images are encrypted using *RSA* algorithm using p and q rounds of execution respectively. Cipher images are generated using *XOR* operations on encrypted plain and secret images. To show the effectiveness of the proposed system, *NPCR* and *UACI* metric have been calculated for five text images for five rounds of different combinations of p, q and r.

In image authentication method, we proposed a hashing based image authentication algorithm for colour images using *DWT* and log-polar transforms. By XORing the *DWT* with the log-polar transform, we better take account into the three image colour planes and the resulting hash is more robust to rotation attacks from the attackers and also to common image content preserving operations. The various parameters have been determined to check the quality of algorithm by means of intensive experiments on a large image data set so as to establish good tradeoffs in content preserving operations in terms of hash robustness against average filtering and large angle rotation attacks. And also show the good sensitivity to the unauthorized image content alterations by changing the position of hash matrix by just 1 column. Compared to the other hashing technique our scheme provides the overall a better performance.

As the future work, we will focus on designing a new robust hashing scheme which can locate tampered regions using the hash matrix of an image as well as to determine the type of the tampering in the image.

References

[1] Agnew G., Mullin R. and Vanstone S., "*An implementation of elliptic curve cryptosystems*", IEEE Journal on Selected Areas in Communications, Vol. 11, No. 4, pp. 804-813, 1993.

[2] Ahmed F., Siyal M., Abbas V.U., "*A secure and robust hash-based scheme for image authentication*," Signal Processing, Vol. 90, No. 5, pp. 1456–1470, 2010.

[3] Alvarez G. and Li S., "*Breaking an encryption scheme based on chaotic baker map*," Physics Letters A, Vol. 352, No. 1-2, pp. 78–82, 2006.

[4] Alvarez G. and Li S., "*Some basic cryptographic requirements for chaos-based cryptosystems*," International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, Vol. 16, No. 8, pp. 2129–2151, 2006.

[5] Arnold V. I., Avez A., "*Ergodic Problem of Classical Mechanics*," in Mathematic Physics Monograph Series, New York, 1968.

[6] Battiato S., Farinella G.M., Messina E., Puglisi G., "*A robust forensic hash component for image alignment,"* Image Analysis and Processing–ICIAP, Springer, pp.473–483, 2011.

[7] Battiato S., Farinella G.M., Messina E., Puglisi G., "*Robust image alignment for tampering detection*," IEEE Transaction Information Forensics Security, Vol. 7, No. 4, pp. 1105–1117, 2012.

[8] Buchmann J. A., "*Introduction to Cryptography*", Second Edition, Springer, 2011.

[9] Cannons J., Moulin P., "*Design and statistical analysis of a hash-aided image watermarking system*," IEEE Transaction Image Proceedings, Vol. 13, No. 10, pp. 1393–1408, 2004.

[10] Chen B. J., Coatrieux G., Chen G., Sun X. M., Coatrieux J. L., Shu H. Z., "*Full 4-D quaternion discrete Fourier transform based watermarking for color images*," Digital Signal Processing, Vol. 28, No. 1, pp. 106–119, 2014.

[11] Chen J., Zhu Z., Fu C., Yu H., and Zhang L., "*A fast chaos based image encryption scheme with a dynamic state variables selection mechanism*," Communications in Nonlinear Science and Numerical Simulation, Vol. 23, No. 4,

pp. 78–88, 2014.

[12] Dang P. P. and Chau P. M., "*Image encryption for secure internet multimedia applications*", IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp. 395, 2000.

[13] Denning D. E., "*Digital Signature with RSA and Other Public-Key Cryptosystems"*, Communications of the ACM, Vol. 27, No. 4, pp. 388-392, 1984.

[14] Dhull S., Beniwal S. and Kalra P., "*Polyalphabetic Cipher Techniques Used For Encryption Purpose*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, No. 2, 2013.

[15] Diffie W. and Hellman M. E., "*New directions in cryptography"*, IEEE Transaction on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976.

[16] ElGamal T., *"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"*, IEEE Transaction on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.

[17] Ell T. A., Sangwine S. J., "*Hyper complex Fourier transforms of color images*," IEEE Transaction Image Proceedings, Vol. 16, No. 1, pp. 22–35, 2007.

[18] Ell T. A., "*Quaternion-Fourier transforms for analysis of two-dimensional linear time invariant partial differential system*," in Proceedings of the 32nd IEEE Conference on Decision Control, pp.1830–1841, 1993.

[19] Fouda J. S. A., Effa J. Y., Sabat S. L. and Ali M., "*A fast chaotic block cipher for image encryption*," Communications in Nonlinear Science and Numerical Simulation, Vol. 19, No. 3, pp. 578–588, 2014.

[20] Fridrich J., Goljan M., "*Robust hash functions for digital watermarking*," in Processing IEEE International Conference on Information Technology, pp.178–183, 2000.

[21] Fu C., Lin B., Miao Y., Liu X., and Chen J., "*Anovel chaos-based bit-level permutation scheme for digital image encryption*," Optics Communications, Vol. 284, No. 23, pp. 5415–5423, 2011.

[22] Gao H., Zhang Y., Liang S., and Li D., "*A new chaotic algorithm for image encryption*," Solitons and Fractals, Vol. 29, No. 2, pp. 393–399, 2006.

[23] Guan Z., Huang F., and Guan W., "*Chaos-based image encryption algorithm*," Atomic and Solid State Physics, Vol. 346, No. 1–3, pp. 153–157, 2005.

[24] Henon M., "*A two-dimensional mapping with a strange attractor*," Communications in Mathematical Physics, Vol. 50, No. 1, pp. 69–77, 1976.

[25] Horst F., "*Cryptography and Computer Privacy*," Scientific American, Vol. 228, No. 5, pp. 15-23, May 1973.

[26] Kantor I .L. V., Solodovnikov A.S., Shenitzer A., "*Hypercomplex Numbers, An Elementary Introduction to Algebras*," Springer Verlag, New York, 1989.

[27] Kozat S.S., Venkatesan R., Mihçak M.K., "*Robust perceptual image hashing via matrix invariants*," in Processing the IEEE International Conference on Image Processing, Singapore, pp.3443–3446, 2004.

[28] Lang F. n., Zhou J. l., Cang S., Yu H., Shang Z., "*A self adaptive image normalization and quaternion PCA based color image watermarking algorithm*," Expert System Application, Vol. 39, No. 15, pp. 12046–12060, 2012.

[29] Laradji I. H., Ghouti L., Khiari E. H., "*Perceptual hashing of color images using hyper complex representations*," in proceedings of IEEE International Conference on Image Processing, ICIP, pp. 4402–4406, 2013.

[30] Lei Y., Wang Y., Huang J., "*Robust image hash in Radon transform domain for authentication*," Signal Processing Image Communication, Vol. 26, No. 6, pp. 280–288, 2011.

[31] Liu F., Cheng L.M., Leung H.Y., Fu Q.K., "*Wave atom transform generated strong image hashing scheme*," Optical Communication, Vol. 285, No. 24, pp. 5008–5018, 2012.

[32] Liu Y., Wu F., Yang Y., Zhuang Y.T., Hauptmann A.G., "*Spline regression hashing for fast image search*," in IEEE Transaction Image Proceedings, Vol. 21, No. 10, pp. 4480–4491, 2012.

[33] Li C., Liu Y., Xie T., and Chen M. Z. Q., "*Breaking a novel image encryption scheme based on improved hyper chaotic sequences*," Nonlinear Dynamics. An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems, Vol. 73, No. 3, pp. 2083–2089, 2013.

[34] Li C., Zhang L. Y., Ou R., Wong K. W., and Shu S., "*Breaking a novel colour*

image encryption algorithm based on chaos, Nonlinear Dynamics", An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems, Vol. 70, No. 4, pp. 2383–2388, 2012.

[35] Li Y., Lu Z., Zhu C., Niu X., "*Robust image hashing based on random Gabor filtering and dithered lattice vector quantization*," IEEE Transaction Image Proceedings, Vol. 21, No. 4, pp. 1963–1980, 2012.

[36] Lütkenhaus N., "*Security against Eavesdropping in Quantum Cryptography*," Phys. Rev., Vol. 54, pp. 97-111, 1996.

[37] Lu W., Wu M., "*Multimedia forensic hash based on visual words*," in IEEE International Conference on Image Processing, ICIP, pp.989–992, 2010.

[38] Lv X., Wang Z.J., "*Perceptual image hashing based on shape contexts and local feature points*," IEEE Transaction Information Forensics Security, Vol. 7, No. 3, pp. 1081–1093, 2012.

[39] Mandal A. K., and Parakash C., "*Performance Evaluation of Cryptographic Algorithms: DES and AES "*, Students' Conference on Electrical, Electronics and Computer Science, pp.1-5, 2012.

[40] Matthews R., "*On the derivation of a "chaotic" encryption algorithm*", Cryptologia, Vol. 13, No. 1, pp. 29–42, 1989.

[41] Monga V., Mhcak M., "*Robust and secure image hashing via nonnegative matrix factorizations*," IEEE Transaction Information Forensics Security, Vol. 2, No. 3, pp. 376–390, 2007.

[42] Nag A., Singh J. P., Khan S., Ghosh S., Biswas S., Sarkar D. and Sarkar P. P., "*Image Encryption Using Affine Transformation and XOR Operation*", International Conference of Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), pp. 309-312, 2011.

[43] Pei S. C., Domg J. J., Chang J.H., "*Efficient implementation of quaternion Fourier transform, convolution, and correlation by 2-D complex FFT*," IEEE Transaction Signal Proceedings, Vol. 49, No. 11, pp. 2783–2797, 2001.

[44] Qin C., Chang C.C., Tsou P.L., "*Robust image hashing using non-uniform sampling in discrete Fourier domain*," Digital Signal Proceedings, Vol. 23, No. 2, pp. 578–585, 2013.

[45] Rivest R. L., Shamir A. and Adleman L., "*A method for obtaining digital signatures and public-key cryptosystems*", in Communication of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[46] Roover C.D., Vleeschouwer C.D., Lefèbvre F., Macq B., "*Robust video hashing based on radial projections of key frames*," IEEE Transaction Signal Proceedings, Vol. 53, No. 10, pp. 4020–4037, 2005.

[47] Sangwine S. J., "*Fourier transforms of color images using quaternion or hypercomplex, numbers"*, Electron. Lett., Vol. 32, No. 21, pp. 1979–1980, 1996.

[48] Senthil K., Prasanthi K., and Rajaram K., "*A Modern Avatar of Julius Ceasar and Vigenere Cipher*", International Conference on Computational Intelligence and Computing Research, pp. 1-3, 2013.

[49] Sethi N. and Sharma D., "*A New Cryptology Approach for Image Encryption*", in 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, pp. 905-908, 2012.

[50] Soleymani A., Nordin M. J. and Sundarajan E., "*A chaotic cryptosystem for image based on henon and arnold map*", Hindawi Publication Corporation, Vol. 11, No. 4, pp. 804-813, 1993.

[51] Stalling W., "*Network Security Essentials (Applications and Standards)*", Pearson Education, 2004.

[52] Stanoyevitch A., "*Introduction to Cryptography with Mathematical Foundations and Computer Implementations*", CRC Press ,2011.

[53] Swaminathan A., Mao Y., Wu M., "*Robust and secure image hashing,"* IEEE Transaction Information Forensics Security, Vol. 1, No. 2, pp. 215–230, 2006.

[54] Tang Z., Dai Y., Zhang X., Huang L., Yang F., "*Robust image hashing via color vector angles and discrete wavelet transform*," IEEE Image Proceedings, Vol. 8, No. 3, pp. 142–149, 2014.

[55] Tang Z., Zhang X., Dai Y., Lan W., "*Perceptual image hashing using local entropies and DWT,"* Imaging Science, Vol. 61, No. 2, pp. 241–251, 2013.

[56] Tang Z., Zhang X., Huang L., Dai Y., "*Robust image hashing using ring based entropies*," Signal Processing, Vol. 93, No. 7, pp. 2061–2069, 2013.

[57] Tang Z., Zhang X., Huang L., Dai Y., "*Robust perceptual image hashing based*

on ring partition and NMF," IEEE Transaction Knowledge Data Engineering, Vol. 26, No. 3, pp. 711–724, 2014.

[58] Tsuim T. K., Zhang X. P., Androutsos D., "*Color image watermarking using multidimensional Fourier transforms*," IEEE Transaction Information Forensics Security, Vol. 3, No. 1, pp.16–28, 2008.

[59] Wang Q., Wang Z., "*Color image registration based on quaternion Fourier transformation*," Optical Engineering, Vol. 51, No. 5, pp. 57001–57008, 2012.

[60] Wang S., Zhang X., "*Attacks on perceptual image hashing*," in Proceedings of 2nd International Conference on Ubiquitous Information Technologies and Applications, pp. 199–203, 2007.

[61] Wang X., Teng L., and Qin X., "*A novel colour image encryption algorithm based on chaos*," Signal Processing, Vol. 92, No. 4, pp. 1101–1108, 2012.

[62] Wang X., Yang L., Liu R., and Kadir A., "*A chaotic image encryption algorithm based on perceptron model,"* Nonlinear Dynamics, Vol. 62, No. 3, pp. 615–621, 2010.

[63] Wu D., Zhou X., Niu X., "*A novel image hash algorithm resistant to print scan," Signal Processing*, Vol. 89, No. 12, pp. 2415–2424, 2009.

[64] Xiang S., Kim H.J., Huang J., "*Histogram based image hashing scheme robust against geometric deformations*," in Proceedings of the 9th Workshop on Multimedia & Security, pp.121–128, 2007.

[65] Xiang T., Liao X., Tang G., Chen Y. and Wong K., "*A novel block cryptosystem based on iterating a chaotic map*," Physics Letters A: General, Atomic and Solid State Physics, Vol. 349, No. 1–4, pp. 109–115, 2006.

[66] Xiao D., Liao X., and Wei P., "*Analysis and improvement of a chaos-based image encryption algorithm*," Solitons and Fractals, Vol. 40, No. 5, pp. 2191–2199, 2009.

[67] Xu S. J., Chen X. B., Zhang R., Yang Y. X., and Guo Y. C., "*An improved chaotic cryptosystem based on circular bit shift and XOR operations*," Physics Letters A, Vol. 376, No. 10-11, pp. 1003–1010, 2012.

[68] Zhang Y., Li C., Li Q. and Zhang D., "*Breaking a chaotic image encryption algorithm based on perceptron model,"* Nonlinear Dynamics, Vol. 69, No. 3, pp.

1091–1096, 2012.

[69] Zhao Y., Wang S., Zhang X., Yao H., *"Robust hashing for image authentication using Zernike moments and local features,"* IEEE Transaction Information Forensics Security, Vol. 8, No. 1, pp. 55–63, 2013.

[70] Zhu C., *"A novel image encryption scheme based on improved hyperchaotic sequences,"* Optics Communications, Vol. 285, No. 1, pp. 29–37, 2012.

[71] Zhu X., Huang Z., Cheng H., Cui J., Shen H. T.," *Sparse hashing for fast multimedia search,"* ACM Transaction Information System, Vol. 31, No. 2, pp. 1–24, 2013.

Communicated Papers

1. Vinay Kumar Verma and Singara Singh Kasana, “A multilevel Hybrid Chaotic Cryptosystem for Digital Images”, Journal of Information Processing Systems, Scopus Indexed.
2. Vinay Kumar Verma and Singara Singh Kasana, “Hashing based Image Authentication using Multiple Transforms”, International Journal of Science and Engineeing, Scopus Indexed.

Video Presentation

.

Below is the link of my video presentation which you can watch on YouTube.

http://youtu.be/ItIs2b_XhPI.