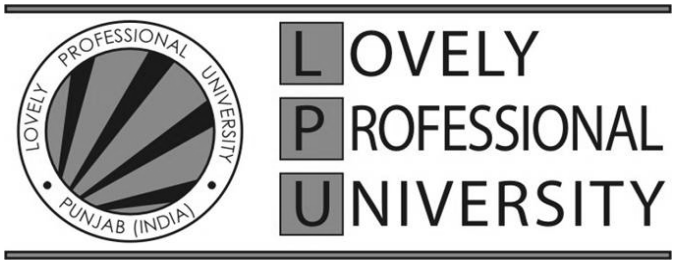

DESIGN AND EVALUATION OF NEW ALGORITHM BASED ON CHAOTIC CRYPTOGRAPHY

A Dissertation submitted

By Praveen Pandey

To

Department of Computer Science and Engineering

In partial fulfillment of the requirement for the

Award of the degree of

Master of technology in CSE

Under the guidance of

Er. Gulshan Kumar

(Advisor)

June, 2015

INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of: Technology & Sciences

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Praveen Pandey Registration No: 11003991

Batch: 2010-15 Roll No. 2001

Session: 2014-15 Parent Section: K1605

Details of Supervisor: Designation: A.P

Name: Gulshan Kumar Qualification: M.Tech

U.ID: 16865 Research Experience: 3 year

SPECIALIZATION AREA: Network Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Design & Evaluation of Asymmetric cryptographic algorithm
2. Design & Evaluation of new algorithm based on chaotic cryptography
3. Modifications in AES algorithm to enhance security

Gkumar 16865
Signature of Supervisor

PAC Remarks: Topic 2 is approved

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 19/9/14

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

With the increase in the communication techniques, people throughout the world are connected to each other through internet. But the data transmitted through internet needs to be protected from the intruders. If the data is not protected, intruders may misuse other's personal data. But images are being misused too. Therefore it is important to protect the images being shared. If the image is converted into some incomprehensible form then there are less chances of misuse. Hence In this research, image is encrypted using IDEA (International Data Encryption Algorithm). First the image is divided into different parts and then DWT is applied. Application of DWT results in confusion of pixels i.e. pixels get jumbled due to which it is impossible to depict the original image. This procedure increases security of the image transmission and helps to reduce the computational delay. So the research involves six phases: division of the image phase, application of DWT, encryption by IDEA, decryption by inverse IDEA, inverse DWT and finally combination phase.

CERTIFICATE

This is to certify that **PRAVEEN PANDEY** has completed M.Tech dissertation titled **DESIGN AND EVALUATION OF NEW ALGORITHM BASED ON CHAOTIC CRYPTOGRAPHY** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.
The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science and engineering.

Date: _____

Signature of Advisor

Name:

ACKNOWLEDGEMENT

Gratitude cannot be seen or expressed. It can only be felt in the heart and is beyond description. Often words are inadequate to serve as a model of expression of one's feeling, specially the sense of indebtness and gratitude to all those who helped in our duty.

It is of immense pleasure and profound privilege to express my gratitude and indebtness along with sincere thanks to **Mr. Gulshan Kumar** for providing me the opportunity to work for the thesis on **DESIGN AND EVALUATION OF NEW ALGORITHM BASED ON CHAOTIC CRYPTOGRAPHY.** During the entire training, I have received endless help from him.

I want to formally acknowledge my sincere gratitude to all those who has assisted and guided me in completing this work. I am beholden to my family and friends for their blessings and encouragement.

PRAVEEN PANDEY

11003991

DECLARATION

I hereby declare that Dissertation entitled **DESIGN AND EVALUATION OF NEW ALGORITHM BASED ON CHAOTIC CRYPTOGRAPHY** submitted for the M.Tech degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Investigator

Registration Number

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1
INTRODUCTION

With the increase in the communication techniques, people throughout the world are connected to each other through internet. But the data transmitted through internet needs to be protected from the intruders. If the data is not protected, intruders may misuse other's personal data. Therefore it is important to protect the images being shared. If the image is converted into some incomprehensible form then there are less chances of misuse.

Image Encryption is the process of converting an image into the unreadable form. While communication images are not secure, intruder may reveal the secret information send by sender. Many new technologies and algorithms are used to hide or secure images. Several algorithms used to protect images are AES, DES, RSA, ECC, etc. This report tells about the image encryption technique using IDEA algorithm.

IDEA is used to make our data encrypted. We want the data to be more secure and unauthorized person cannot access the data. So in order to protect data, cryptography provides two methods to secure our data using symmetric method and asymmetric method. In symmetric method similar key is utilized for encryption as well as decryption and in asymmetric key method unique keys are utilized for purpose of encryption as well as decryption.

Here, image can use 128 bit encoder for encryption and decryption of the image. In this 128 bit data is divided into 128 bits and these are then divided into 4*4 array. In AES we have rounds according to the bit size of data to encrypt an image. Hence In this research, image is encrypted using IDEA (International Data Encryption Algorithm). First the image is divided into different parts and then DWT is applied. Application of DWT results in confusion of pixels i.e. pixels get jumbled due to which it is impossible to depict the original image. This procedure increases security of the image transmission and helps to reduce the computational delay. This procedure increases security of the image transmission and helps to reduce the computational delay. So the research involves six phases: division of the image phase, application of DWT, encryption by IDEA, decryption by inverse IDEA, inverse DWT and finally combination phase.

1.1 DISCRETE WAVELET TRANSFORMATION

Wavelets are numerical capacities that cut up information into different recurrence segments, and afterward examine every part with a determination coordinated to its scale. They have focal points over conventional Fourier systems in breaking down physical circumstances where the sign contains discontinuities and sharp spikes. Wavelets were produced autonomously in the fields of math, quantum material science, electrical designing, and seismic topography. Trades between these fields amid the most recent ten years have prompted numerous new wavelet applications, for example, picture pressure, turbulence, human vision, radar, and seismic tremor expectation. This paper acquaints wavelets with the intrigued specialized individual outside of the computerized sign preparing field. I portray the historical backdrop of wavelets starting with Fourier, contrast wavelet changes and Fourier changes, state properties what's more, other uncommon parts of wavelets, with some fascinating applications, for example, picture pressure, musical tones, and de-noising the data. In this the wavelets of DWT are discretely sampled [26], it is much better than discrete Fourier transformation in respect of temporal resolution that is it captures the data in both frequency as well as location domain. Wavelet is used as an advanced version to Fourier decomposition which is the classical one. Wavelets are also used to remove various kinds of noises from the music recordings. The discrete wavelet transform has countless uses in science, designing, math as well as software engineering. It is utilized for sign coding to show discrete signal in repetitive structure for preconditioning information compression [26]. Commonsense applications are sign preparing of increasing accelerators for step analysis, in advanced communication and numerous others. The essential thought behind wavelets is to dissect as per scale. For sure, a few analysts in the wavelet field feel that, by utilizing wavelets, one is receiving an entire new mentality or viewpoint in transforming information. Wavelets are capacities that fulfill certain scientific prerequisites and are utilized as a part of speaking to information or different capacities. This thought is not new. Close estimation utilizing superposition of capacities has existed following the mid 1800's, when Joseph Fourier found that he could superpose sines and cosines to speak to different capacities. On the other hand, in wavelet investigation, the scale that we use to take a gander at information assumes an uncommon part. Wavelet calculations process information at different scales or resolutions. On the off chance that we take a gander at a sign with an extensive window," we

would notice gross highlights. Also, in the event that we take a gander at a signal with a little window," we would perceive little highlights. The outcome in wavelet investigation is to see both the woods and the trees, as it were. This makes wavelets intriguing and helpful. For a long time, researchers have needed more proper capacities than the sines and cosines which contain the bases of Fourier investigation, to estimated wild flags. By their definition, these capacities are non-neighborhood (and extend to infinity). They along these lines make an extremely poor showing in approximating sharp spikes. Anyhow, with wavelet investigation, we can utilize approximating capacities that are contained conveniently in finite areas. Wavelets are appropriate for approximating information with sharp discontinuities.

The wavelet investigation system is to receive a wavelet model capacity, called a breaking down wavelet or mother wavelet. Worldly investigation is performed with a contracted, high-recurrence variant of the model wavelet, while recurrence investigation is performed with a widened, low-recurrence variant of the same wavelet.

Wavelet investigation [20] is energizing new technique for taking care of troublesome issues in arithmetic, material science, as well as designing, with present day applications such as propagation of wave, information compression, processing of images, recognition of patterns, PC design, location of flying machine as well as submarines as well as other therapeutic picture innovation. Wavelets permit complex data, such as, music, discourse, pictures, etc.

To divide or convert into smaller forms at various positions Signal transmission is taking into account transmission of progression of numbers. Arrangement representation of capacity is vital for wide range of sign transmission. Wavelet representation of capacity is another procedure. Wavelet transform is updated variant of Fourier transform. Fourier transform is capable instrument for dissecting segments of stationary sign. In any case, it is fizzled for examining non stationary signal where as wavelet transform permits parts of non-stationary sign to be broke down.

The Alfred Haar [26] a mathematician has represented the by the 2^n which means it simply pair the values. Also the more new version of dwt is dual tree complex wavelet transformation. It can be used as function to encrypt the image and also for the decryption process. The dwt uses reoccurrence relation in order to make finer discrete sample. This can be performed in O(n) and it also uses to capture the frequency data from the input. It is a

function which represents the signal in invariant to the shift of time. We can use it to generate the signal coding. The wavelet has many applications [20] like:-

1. Processing the signal
2. Compression of the data.
3. To verify the fingerprint.
4. Removing noises and smoothing it.
5. Analyzing the DNA
6. Recognizing the speech.
7. Analyzing various computer graphics
8. Analyzing the blood pressure
9. The heart rate.
10. In describing the internet traffic.
11. In biology or determining cell membranes
12. In pathological labs
13. Analysis of DNA
14. Analysis of proteins
15. For detecting rapid changes in values
16. Innumerable areas in physics

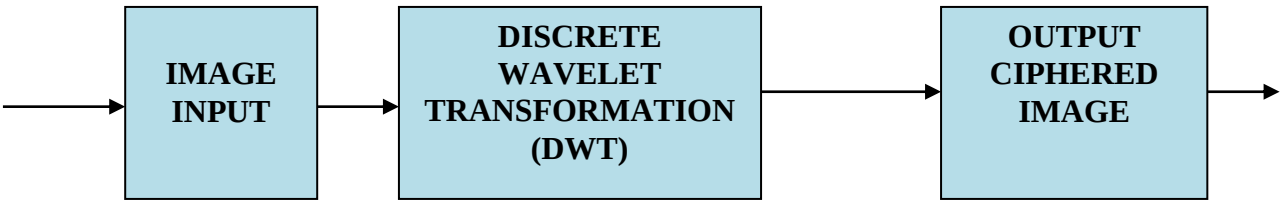

Fig. 1.1.1 DWT layout

FBI (Federal Bureau of Investigation) [20] in USA employs wavelets as device to keep in table fingerprints electronically. For long time, FBI put away their fingerprints in paper design in much secured building located inside Washington; they filled region which had same size to football ground. In event that one expected to contrast a finger impression in San Francisco as well as put away fingerprints, one needed to mail it to Washington.

Moreover, correlation of the fingerprints was basically done physically, so it was the moderate methodology. Thus, FBI began to look for approaches to store fingerprints electronically; this would encourage transmission of data as well as inquiry in chronicle.

1.2. CHAOTIC FUNCTION

These are the functions which are used to create random pixel substitution these are very sensitive to the changes which has been done i.e. even minute change in the image will be known by this function. They produce the precise image as it is very deterministic. Chaotic functions mainly want:

a) Whole function representation
b) Point of global maximum

Sin (1/x) is used to find the point of global optima.

Different types of chaotic maps are [27]:

- Arnold's cat map
- Baker's map
- Bogdanov map
- Chen-lee system
- Circle map
- Complex squaring map
- Complex quadratic map
- Complex cubic map
- Duffing map
- Duffing equation
- Horse shoe map
- Gauss map
- Logistic map
- Lozi map
- Tent map, etc.

These maps are generally augmented by discrete time argument and continuous time parameter. Chaotic maps are generally made by the fractals and these fractals are made by the iterative procedure. Chaos theory is used in all fields such as sociology, physics, biology,

mathematics, etc. Chaos theory is also used in science related fields to determine future such as weather and climatic conditions.

The time of prediction depends on:

- Uncertainty
- Accuracy
- Time scale

Information compression might be lossy as well as lossless is obliged to reduce the storage necessity as well as better information transfer rate. Picture compression system is best when utilized wavelet transform. It is new concept as well as has numerous merits over others. Wavelet transform utilizes a vast mixed bag of wavelets for disintegration of pictures.

1.3 SECURING SENSITIVE INFORMATION

While the Web postures new difficulties in data security, a large number of them can be tended to by the conventional stockpile of security instruments:

- Solid client verification to recognize clients
- Granular access control to cutoff what clients can see and do
- Examining for responsibility
- System encryption to ensure the classification of touchy information in transmission

1.4 ENCRYPTION

Encryption is an essential part of a few of these arrangements. For instance, Secure Attachments Layer (SSL), a Web standard system encryption and verification convention, utilizes encryption to emphatically confirm clients by method for X.509 computerized declarations.SSL likewise utilizes encryption to guarantee information privacy, and cryptographic checksums to guarantee information respectability. Large portions of these employments of encryption are generally straightforward to a client or application. For instance, numerous programs bolster SSL, and clients by and large don't have to do anything unique to empower SSL encryption.

While encryption is not a security cure-all, it is a vital device in tending to particular security dangers. Specifically, the quick development of e-business has prodded expanded encryption of put away information, for example, MasterCard numbers. While SSL is normally utilized

ensure these numbers in travel Site, information not secured as it away, document framework or database putting away them frequently does as such as clear content (un-encoded). Data put away free is then straightforwardly available to any individual who can break into the host as well as addition root get to, or increase illegal access 2 database. Databases are made very secure through legal setup; however they can likewise be helpless against host break-ins if host is misconfigured. In very much broadcasted break-ins, programmer acquired vast rundown of Visa numbers by breaking in database. Had they been encoded, the stolen data would have been futile. Encryption of put away information can consequently be critical instruments in constraining data misfortune even in the typically uncommon event that get to controls are avoided. The diagram of encryption and decryption process is as follows [28]:

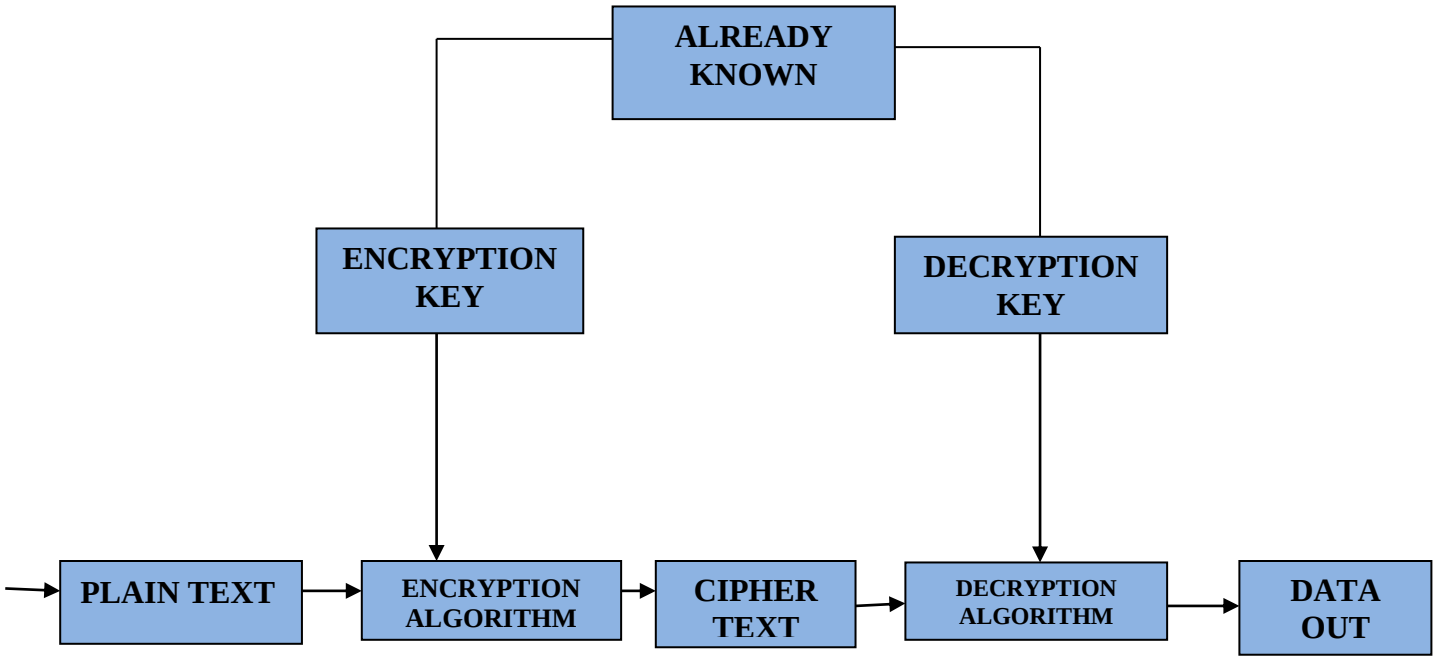

Fig. 1.4.1 Encryption and Decryption

1.4.1 ENCRYPTION DOES NOT TACKLE ACCESS CONTROL ISSUES

Most associations need to cutoff information access to the individuals who have a "need to know." for instance, a HR framework may confine workers to review just their own business records, while permitting administrators of representatives to see the livelihood records of subordinates [29]. HR authorities might likewise need to see representative records for

different representatives. This sort of security strategy -restricting information access to those with a need to see it -is ordinarily tended to by access control systems. The Prophet database has given solid, freely assessed access control instruments for a long time. It empowers access control implementation to a greatly fine level of granularity, through its Virtual Private Database ability.

Since HR [29] records are viewed as delicate data, it is enticing to feel that all data ought to be encoded "for better security." Notwithstanding, encryption can't implement granular access control, and it might really ruin information access. Case in point, a worker, his administrator, and a HR assistant may all need to get to the representative's record. In the event that all representative information is scrambled, then every one of the three must have the capacity to get to the information in un-encoded structure. Consequently, the worker, the administrator and the HR assistant would need to have the same encryption key to unscramble the information. Encryption would hence not give any extra security in the feeling of better get to control, and the encryption may really block the best possible or productive working of the application. An extra issue is that it is extremely hard to safely transmit and offer encryption keys among different clients of a framework.

A fundamental guideline behind scrambling put away information is that it should not meddle with access control [29]. For instance, a client who has SELECT benefit on EMP ought not to be constrained by the encryption system from seeing all the information he is generally permitted to see. Additionally, there is little advantage to scrambling piece of a table with one key and some piece of a table with another key if clients need to see all encoded information in the table; it only adds to the overhead of unscrambling the information before clients can read it. If in case that get to controls are executed well, encryption includes minimal extra security inside the database itself. Any client who has benefit to get to information inside the database has no more or any less benefit as a consequence of encryption. Thusly, encryption ought to never be utilized to take care of access control issues.

1.4.2 ENCODING EVERYTHING DOES NOT MAKE INFORMATION SECURE

A typical slip is to feel that if encoding some information fortifies security, then scrambling everything makes all information secure [29]. As the dialog of the former two standards

shows, encryption does not address access control issues well, and it is imperative that encryption not meddle with typical access controls. Besides, encoding a whole generation database implies that all information must be decoded to be perused, upgraded, or erased. Encryption is innately an execution escalated operation; scrambling all information will fundamentally influence execution.

Accessibility is a key part of security [29]. In the event that encoding information makes information inaccessible, or unfavorably influences accessibility by lessening execution, then scrambling everything will have made another security issue. Accessibility is likewise unfavorably influenced by the database being distant when encryption keys are changed, as great security practices require all the time. At the point when the keys are to be changed, the database is out of reach while information is decoded and re-scrambled with another key or keys. Notwithstanding, there may be points of interest to scrambling information put away logged off. Case in point, an association may store reinforcements for a time of six months to a year disconnected from the net, in a remote area. Obviously, the first line of insurance is to secure the office putting away the information, by securing physical access controls. Encoding this information before it is put away may give extra advantages. Since it is not being gotten to on-line, execution require not be a thought. While a Prophet Database server does not give this ability, there are merchants who can give such encryption administrations. Before setting out on substantial scale encryption of reinforcement information, associations considering this methodology ought to completely test the procedure. It is vital to check that information scrambled before logged off capacity can be decoded and re-imported effectively [29].

When Internet is utilized by users, users not generally simply clicking around and passively getting an information, for example, reading articles or blog entries - a maximum of their time online involves sending others their own particular/personal information. Ordering something over the Internet, whether book, a CD or whatever else from online vendor requires entering of sensitive personal information. A common transaction may not include just the names, e-mail ids and physical addresses and phone/mobile number, additionally passwords as well as personal identification numbers (PINs) [30].

The incredible development of Internet has raised businesses as well as consumers with its promise of modifying way they live as well as work. It's easy to purchase as well as sell

merchandise everywhere throughout world by sitting before tablet. Be that as it may, security significant concern on Internet, when you're utilizing it for sending sensitive information to other parties [30].

Data security is on PCs [30] as well as over Internet by mixed bag of strategies. A straightforward as well as clear security strategy is to keep touchy data on removable storage media like portable memory drives or other hard drives. Most famous type of security all depend on encryption, methodology of encoding data in such path, to point that just individual with key can decipher it.

1.5 IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM)

IDEA is 64-bit block transformation with 128-bit keys presented by Lai as well as Massey in 1991. IDEA is standout amongst the most broadly utilized square figures, because of its consideration in a few cryptographic bundles, for example, PGP. Since its presentation in 1991, IDEA has withstood broad tomb scientific exertion, however no assault was found on the full (8.5-round) variation of the figure. In 2006 Eli Biham, Orr Dunkelman and Nathan Keller present the first known assault on 6-round IDEA quicker than thorough key hunt. The assault abuses the feeble key-plan calculation of IDEA, and joins Square-like strategies with straight cryptanalysis to build the quantity of rounds that can be assaulted. In this paper we are breaking down the execution of IDEA calculation by making adjust variable. By this we are attempting to build the security of IDEA calculation.

The IDEA (International Data Encryption Algorithm):

A) Provides too high security to keep calculation mystery/hidden
B) Yet unending supply of the mystery/secret key is totally decided and successfully
C) gotten on i.e. reasonable
D) is open to all
E) is suitable for utilization in far reaching mixture of applications
F) executed in electronic fragments (VLSI Chip)
G) utilized effectively as well as efficiently
H) may be conveyed throughout world

First encryption round [32], starting 4 16-bit key sub-pieces are united with 2 of 16-bit plaintext squares using expansion modulo 216, as well as with other 2 plain text parts

utilizing expansion modulo 216 + 1. Results are then changed as exhibited in Figure , whereby 2 more 16-bit key sub-squares enter estimation as well as 3rd arithmetical social affair head, small bit if particular OR, is utilized. Around end of 1st encryption cycle 4 16-bit qualities are conveyed which used data to 2nd encryption round are in not entirely changed appeal. System portrayed above for cycle 1 is reiterated in each 7 encryption rounds using unmistakable 16-bit key sub-bytes for each mix. In midst of subsequent yield change, 4 16-bit qualities made toward end of 8th encryption round are solidified with last 4 of 52 key sub-pieces using development modulo 216 as well as duplication modulo 216 + 1 to edge resulting 4 16-bit figure cipher text parts. The matrix figure Thought meets expectations with 64-bit plaintext and figure substance squares and is controlled by 128-bit key. The essential calculations in the diagram of this figuring are the usage of operations from three diverse scientific gatherings. The substitution boxes and the related table lookups used as piece of square figures open to-date [31] have completely kept up a key separation from. The estimation structure has been picked such that, with uncommon case that particular key sub-pieces are used, encryption strategy is indistinguishable to encrypting system. The computational method used for interpreting/decrypting of cipher text is fundamentally the same as that used for encryption of the plaintext. The primary qualification differentiated and encryption is that in midst of decryption/disentangling, particular 16-bit key sub-squares are made. More definitively, each of 52 16-bit key sub-squares used for deciphering is opposite of key sub-square used in midst of encryption as a piece of energy about joined arithmetical get-together operation. Additionally [32], the key sub-pieces must be used as a piece of inverse solicitation in midst of translating to upset encryption process. The structure of IDEA is as follows [32]:

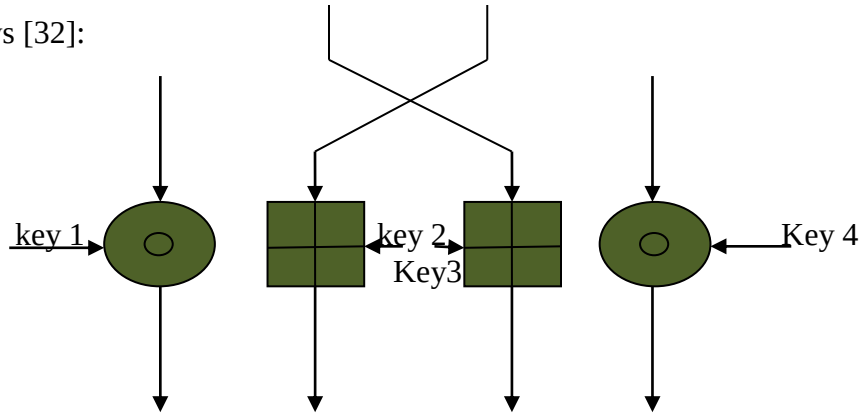

Fig. 1.5.1 IDEA structure

IDEA (International Data Encryption Algorithm) is a piece figure which ever named PES (Proposed Encryption Standard), then the name changed to IPES (Improved PES). Because of its consideration in a few cryptographic bundles, for example, PGP, IDEA is a standout amongst the most generally utilized piece figures. The figure is taking into account the configuration idea of blending operations from diverse arithmetical gatherings". The obliged perplexity is accomplished by progressively utilizing three distinctive gathering operations on sets of 16-bit sub pieces and the figure structure was decided to give the important dissemination. The main idea is constructed to the point that the unraveling procedure is the same as the enciphering process once the decoding key sub pieces have been figured from the encryption key sub squares. The figure structure was decided to encourage both equipment and programming usage. Some have altered the IDEA Algorithm by changing the consistent 8 rounds into variable (n-1) rounds. Client then needs to pass two contentions:

- Key.
- No. of rounds.

In public key cryptosystems there are two distinct keys: a public key, which is publicly known, and the secret key, which is kept secret by the proprietor. The framework is called "asymmetric" following the distinctive keys are utilized for encryption. On the off chance that information is encoded with a public key, it must be unscrambled utilizing the relating private key, and the other way around. The example client key is sustained into key generation for every round module which produces 16 sub-keys in each round. Sample client key is likewise bolstered into shift rationale module that shifts the key by 25 bit circular left shift and again 16 sub-keys are generated. The procedure is completed recursively till each of the 104 sub-keys are produced.

How IDEA works? [32]

- IDEA divides the entire data in chunks of 64 bit blocks
- IDEA works on 64 bit blocks of data
- Each block uses 128 bit key.
- The data is then goes through eight and half rounds to encrypt the data.
- The process of encryption and decryption is same in case of IDEA.
- Modular addition, multiplication and Xoring are the main work of the idea.

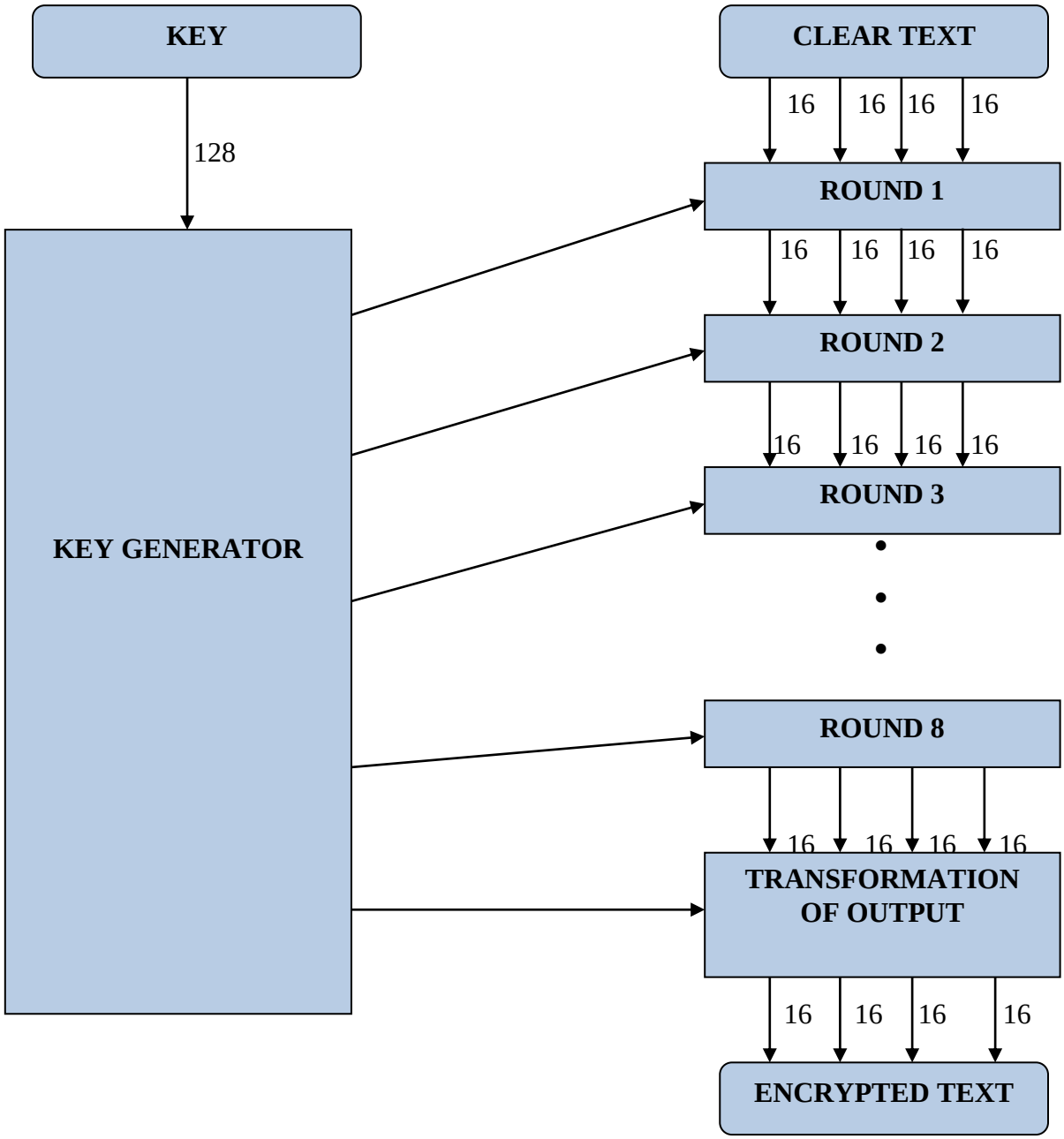

Fig 1.5.2 IDEA Diagram

Steps of IDEA:

1. Multiply Y1 & 1st key W1.
2. Add Y2 & 2nd key W2.
3. Add Y3& 3rd key W3.
4. Multiply Y4 & 4th key W4.
5. XOR steps 1 & 3.
6. XOR steps 2 & 4.
7. Multiply step 5 & 5th key W5.
8. Add steps 6 & 7.
9. Multiply step 8 & 6th key W6.
10. Add steps 7 & 9.
11. XOR steps 1 & 9.
12. XOR steps 3 & 9.
13. XOR steps 2 & 10.
14. XOR steps 4 & 10.

For every round except final ROUND, swap ROUND occurs, input to next round is result of step 11 XOR result of step 13 XOR result of step 12 XOR result of step 14, which becomes X1 XOR X2 XOR X3 XOR X4, input for next round. After round (N-1), final (half round) round occurs:

1. Multiply Y1 & 1st key.
2. Add Y2 & 2nd key.
3. Add Y3 & 3rd key.
4. Multiply Y4 & 4th key.

Julio Cesar hernandez castro (2005) [4] had proposed a model to make data secure by using Artificial Intelligence in which it focuses on Genetic Algorithm and its programming. It focuses on issue of fitness function for the available heuristic methods. It also uses test batteries to be used as fitness function. It also makes us clear that most critical step is substitution box for the development of the block cipher.

N.K. Pareek and et al. (2006) [18] had proposed a method to make the image secure by using logistic map with the help of chaotic technique. In this the image is secured by using eternal hidden key of 80bit in length , later on this 80bit key is divided into several 8 bit. It also used two different logistic maps. It also generate 24 values which are real, these values are obtained by doing various iteration on the initial value. It also analyses the image by statistical and the histogram method. It also focuses on the method that the key space must be large in order to make all the attacks infeasible.

M zeghid et al. (2007) [25] has proposed a new scheme to encrypt image using the modified AES .They have also modified AES by using key stream generator (A5/1, W7) to the AES algorithm so as to increase performance as well as image security. They have also analyzed security by statistical approach. Two further methods are used to analyze security.

i) Histograms of encrypted images

ii) Co-relation of two adjacent pixels.

In former analysis the histogram of ciphered image is uniform which cannot reveal secret information to intruder. Moreover secret key is chosen large enough so that brute force attack is not possible. In the AES algorithm the 7 bit is the input and output which is used in front of 128 bit of AES algorithm. We can also use DES which is Data Encryption Standard but it involves 16 rounds of encryption. This makes code so complex that it becomes difficult to implement the image for encryption and decryption purpose. In DES the key size used is of size 56 and the block size is of 64 and also number of sub-bytes is 16.We can also encrypt the image using chaotic algorithm in which the encryption is done by scattering the image

pixels and then manipulating the image pixel using some chaotic function. Secure image encryption involves 3 main components that are:

i) Horizontal vertical component.

ii) Shift function

iii) Gray scale function.

The models support 2 modes of operation namely Electronic Code Book and Cipher Block Chaining. Finally after doing various experiments they have shown that using W7 key generator has solved the problem of textured zones problem which was coming in other encryption algorithms. Moreover the performance and security has also increased using W7 key generator.

Dinghui, Zhang et al. (2008) [6] introduced a method to encrypt the JPEG image using various techniques it uses the discrete chaotic function in order to get encrypted image this paper also done a good analysis on encryption and decryption of the image which is generated by chaotic encryption. It also created 8*8 block of images which is very fast s compared to other techniques. In this firstly the image is compressed and then that produced image is scrambled in rows and various columns. Decryption is done firstly by decompressing image into three 2 dimensional images. Inverse scrambling is performed on the 8*8 images which are generated earlier.

Dipalee Gupta et al (2008) [10] introduced picture compression is a system through which we can diminish the storage room of pictures which will accommodating to build stockpiling and transmission process' execution. In this paper, we show the examination of the execution of discrete wavelets like Haar Wavelet and Daubechies Wavelet for usage in a still picture pressure framework. The exhibitions of these changes are thought about regarding Mean squared mistake (MSE) as well as Energy Retained (ER) and so on. The principle target is to examine the still picture pressure of a dim scale picture utilizing wavelet hypothesis. This is actualized in programming utilizing MATLAB Wavelet Toolbox and 2D-DWT strategy. The tests and results are done on .jpg arrangement pictures. These outcomes give a decent reference to application engineers to pick a decent wavelet pressure framework for their application. Compression is one of the real picture transforming systems. It is a standout

amongst the most valuable and financially effective advances in the field of computerized picture preparing. Picture pressure is the representation of a picture in computerized structure with as couple of bits as could be allowed while keeping up an adequate level of picture quality. Progressively pictures are obtained and put away digitally or different film digitizers are utilized to change over conventional crude pictures into computerized arrangement. Data pressure is the procedure to diminish the redundancies in information representation keeping in mind the end goal to decline information stockpiling necessities and consequently correspondence costs. Lessening the stockpiling prerequisite is comparable to expanding the limit of the stockpiling medium expand the rate of transmission and thus correspondence bandwidth. The proficient methods for putting away huge measure of information and because of the data transfer capacity and capacity limits, pictures must be compacted before transmission and storage. At some later time, the packed picture is decompressed to reproduce the first picture or rough guess of it. Compression of picture is a vital field in Digital sign transforming. In this paper, examination of different changes based picture pressure system is portrayed. In the event that the vitality held is 100% then the pressure is known as lossless means we effectively restore all the data valuable for client. This happens when the limit worth is situated to zero, implying that the point of interest has not been changed. In the event that any qualities are changed then vitality will be lost and this is known as lossy pressure.

In lossy pressure the data is misfortune, so we not restore all the data. In a perfect world, amid pressure the no of zeros and the vitality maintenance will be as high as could reasonably be expected. In Daubechies wavelet held vitality is 98.03% and in haar change it is 97.70%. So from the outcomes, it has been presumed that Daubechies wavelet change demonstrates the best results as far as Energy Retain as contrast with Haar wavelet change.

Bin Chen et al. (2009) [24] have proposed a model which is based on reversible pair-wise swap-ping technique. In this digital image is used to create a half toning image which is very much popular in printing. In this image is encrypted and decrypted on basis of reversibility. In half toning image which is continuous tone is converted into two toned image. In this 16bit grey level image is changed to 2bit color halftone. Reversible paired swapping has two

elements which are represented by x and y. In decryption images each block is converted to decimal integer matrix.

M. Siffuzzaman et al (2009) [20] Wavelet investigation is an energizing new technique for tackling troublesome issues in arithmetic, material science, and building, with present day applications as differing as wave engendering, information pressure, sign transforming, picture handling, example acknowledgment, PC design, the location of air ship and submarines and other therapeutic picture innovation. Wavelets permit complex data, for example, music, discourse, pictures and examples to be deteriorated into rudimentary structures at diverse positions and scales and thusly reproduced with high accuracy. Signal transmission is in view of transmission of a progression of numbers. The arrangement representation of a capacity is imperative in a wide range of sign transmission. The wavelet representation of a capacity is another procedure. Wavelet change of a capacity is the progressed form of Fourier change. Fourier change is a capable apparatus for breaking down the arts of a stationary sign. In any case, it is fizzled for breaking down the non stationary signal where as wavelet change permits the parts of a non-stationary sign to be investigated. In this paper, our fundamental objective is to figure out the benefits of wavelet change contrasted with Fourier change. The wavelet change is regularly contrasted and the Fourier change. Fourier change is an intense device for breaking down the parts of a stationary sign (a stationary sign is a sign where there is no adjustment in the properties of sign). For case, the Fourier change is a capable apparatus for preparing flags that are made out of some mix of sine and cosine signals (sinusoids) Mallat. The Fourier change is less helpful in examining non-stationary sign (a non-stationary sign is a sign where there is change in the properties of sign). Wavelet changes permit the segments of a non-stationary sign to be dissected. Wavelets likewise permit channels to be developed for stationary and non-stationary signs Wells, Strang. The Fourier change appears in a wonderful number of ranges outside of fantastic sign transforming. Notwithstanding considering this, we imagine that it is safe to say that the arithmetic of wavelets is much bigger than that of the Fourier change. In actuality, the science of wavelets incorporates the Fourier change. The extent of wavelet hypothesis is coordinated by the span of the application zone. Starting wavelet applications included sign transforming and separating. Then again, wavelets have been connected in

numerous different ranges including non-straight relapse and pressure. A branch of wavelet pressure permits the measure of determinism in a period arrangement to be evaluated.

Morris Dworkin et al (2010) [7] is one of the mode upon which AES is implemented. The researchers have provided recommendation for the block cipher mode of AES. Mode is known as key wrap (KW). When the key wrap is done with the padding to provide interoperability then this is known as key wrap with padding (KWP). The triple idea key wrap (TKW) is used to support legacy applications. The above all techniques provide confidentiality as well as integrity to keys as well as data.

Forward transformation is permutation of data is caused by the block cipher in conjunction with the key. The key used in forward transformation is called key encryption key (KEK). The inverse of forward transformation is known as inverse transformation. For key, the wrapping and the unwrapping functions are applied on the 3 or more blocks. But the resulted length of output is same as input for both functions. Prerequisites are KEK and K and 128 bit cipher block. Two types of algorithms are explained for the key wrapping.

The plain text is expanded in the authentication encryption function which provides the authenticity to the data. If the output is a plaintext then the cipher text is authenticated else it is not authenticated.

Dag, Arne, Oswik et al. (2010) [17] Introduced AES is also very useful in platforms like 8-bit microcontrollers to 64 bit processors. They have done research on not only doing secure and efficient implementations of AES but also they have checked the performance of AES algorithm on different architectures. They noticed that smart cards and radio frequency identification tag, RFIDs usage is increasing day by day. Therefore they present new software implementations of AES with very high speed and small code size. They have ported AES to different platforms and accordingly different decisions have been made and also different results were obtained according to the availability of RAM and flash memory. Two variants were created fast and compact. Different components on which AES was implemented were:

- 8-bit AVR microcontroller
- Synergistic processing element
- 32-bit ARM microprocessor

- Graphic processing units.

For first two byte sliced implementations were employed while T-table approach was implemented in next two. Also this was first AES implementation for the graphical processing unit implementing both encryption as well as decryption.

Sandipan Basu (2011) [3] introduced few symmetric and asymmetric information encryption calculations. IDEA (International Data Encryption Algorithm) is one of the strongest mystery key square figures. In this article, they attempt to speak to the current IDEA calculation in an alternate manner. In the accompanying outline, we would perceive how the encryption can be communicated in a more straightforward manner. The IDEA (International Data Encryption Algorithm) is a solid block cipher. Despite the fact that there are numerous operations included in the whole calculation, just three diverse of operations are included. As the figure key size is 128 bits, in that regard IDEA is excessively solid (having taken tend to feeble keys).

Abdul Hanan Abdullah et al. (2012) [1] had proposed a hybrid mode which is used to encrypt the image in this model they have firstly created large number of these images using various chaotic and other techniques and then at the second stage these images are used as initials for the genetic algorithm. In each step the previous one is used to produce the next better encrypted image. Encrypted image is that one which has the highest entropy value. It uses chaotic function and genetic algorithm to produce the encrypted image which is very popular.

Dominik Engel et al. (2012) [8] Encrypted image by predicting that the image is in the form of packets that is energy which is further encrypted with the help of dependent sub-band structure. We analyze their nature in order to know how these images get compressed in order combine with the sub-band structure. In this the image which is encrypted is available in lower quality and in order to get the whole high quality image you need to pay to get the decrypted image. So in this the quality of the image is degraded in order to make the image more secure. In this the JPEG2000 is encrypted using KDWP (key dependent wavelet packet) in a secure way. It is done using 3 ways like In this the quality of the image is

reduced. In this all the concepts on which the transformation takes place is given in this. It takes care of the security of the image.

C.K. Huang and et al. (2013) [12] Introduced gray of image which is not eliminated even after removing the gray level the outline of the image is not removed completely. So to remove such type of outlines chaotic technique in which the picture shuffling is done is combined with the various rows and column shuffling in order to remove the outlines. Also in order to do so we have to use multiple dimension chaotic technique. It also uses correlation coefficient which helps to encrypt the modified image more securely. In this original image is taken then the image is shuffled in both the directions i.e. rows and columns. Then on that image chaotic technique is applied in order to make that image more secure.

Mahajan et al (2013) [15] proposed that there are numerous security calculations that are utilized for security reason. Thought is one of them. The piece figure IDEA works with 64-bit plaintext and figure content pieces and is controlled by a 128-bit key. The principal development in the outline of this calculation is the utilization of operations from three distinctive mathematical gatherings. The calculation structure has been picked such that, with the special case that diverse key sub-pieces are utilized, the encryption methodology is indistinguishable to the decoding methodology. The disadvantage of IDEA is that the substantial quantities of feeble keys were found in IDEA (International Data Encryption Algorithm). Additionally another assault on the cycle six of the IDEA has been recognized. In this paper depict the configuration and usage of secure information encryption algorithm(S-IDEA) convention, the measure of the key has been expanded from 128 bits to 256 bits. This expanded key size will build the unpredictability of the calculation. To build the measure of dispersion two MA pieces (multiplicative added substance piece) are utilized as a part of a solitary round of IDEA as contrasted with one MA square utilized already as a part of a solitary round, with these alterations in the proposed calculation will build the cryptographic quality. The encryption methodology comprises of eight indistinguishable encryption steps (known as encryption rounds) trailed by a yield change. The structure of the first round is indicated in subtle element. In the first encryption round, the initial four 16-bit key sub-pieces are joined with two of the 16-bit plaintext squares utilizing expansion modulo

216, and with the other two plaintext pieces utilizing augmentation modulo 216 + 1. The outcomes are at that point prepared further as indicated, whereby two more 16-bit key sub-squares enter the computation and the third mathematical gathering administrator, the a tiny bit at a time restrictive OR, is utilized. Toward the end of the first encryption cycle four 16-bit qualities are created which are utilized as information to the second encryption round in an in part changed request. The procedure portrayed above for cycle one is rehashed in each of the consequent 7 encryption rounds utilizing diverse 16-bit key sub blocks for every mix. Amid the consequent yield change, the four 16-bit qualities delivered toward the end of the 8th encryption round are consolidated with the last four of the 104 key sub-squares utilizing expansion modulo 216 and duplication modulo 216 + 1 to frame the subsequent four 16-bit figure content squares.

Hermassi, Houcemeddine et al. (2013) [11] proposed better versions of picture cryptosystem by adjusting/modifying S-box as well as P-box of classical cryptography. By applying such modification the brute force attacks reduced and execution of encryption and decoding/decryption has increased. Problems confronted by previous chaotic cryptosystems were that they were not secure to attacks like chosen and known plain text. Two modifications done here are basically to S-Box and P-Box. They made plain text which is in connection with key stream. Therefore, at whatever point plain text changes key stream changes naturally. They used PWLCM map for shuffling which reduces the quantity of iterations to transform the rows as well as columns. Instead of using ECB they utilized CBC in which every plain text block gets Xored with previously used ciphered data block.

Security was broke down using co-connection of adjoining pixels and histograms. In any case, the issue still exists in generation of key and in the permutation process. At last they concluded that attacker will be more confused when user will take the above described method. Subsequently it has shown better execution as contrast with DES, AES and triple DES.

Joan daemen and Craig clap (2013) [5] Introduced PANAMA which is used as a module that can be used in cryptographic hash function as well as stream cipher. They have shown that very fast implementations of software can be done using inherent parallelism on VLIW processor. Panama is based on a machine which uses 8192 buffer and 544 bit state. These 2 are updated by using iterations. Panama uses hermetic hash function which must include:

- The expected workload of generating a collision is of the order of 2^ (n/2).
- If the n bit values are given then the expected workload of finding the message is 2^n executions of the hash function.
- When messages and its hash value is given then expected workload of finding the second message is of the order of 2^n executions of the hash function.

Panama is also K-secure if a key stream output along with a given key and chosen value of q is given then the effective way to get the knowledge of the key can be done by doing exhaustive search. The future scope of panama is that it will be used in set top boxes and digital televisions which will be used in the future because they require media processors for decompressing the video and for performing various other tasks. The panama gives high data rates and performance.

Vijayvargiya et al. (2013) [22] Scrambled pictures from multiple points of view; a few procedures have utilized diverse encryption techniques. In this exploration, we apply another adjusted International Data Encryption Algorithm to scramble the full picture in an effective secure way, after encryption the first document will be divided and changed over to another picture records. By utilizing Huffman Algorithm the divided picture records are blended. What's more, we union the whole sectioned picture to pack into a solitary picture? At long last we recover a completely unscrambled picture. Next we locate a proficient approach to exchange the scrambled pictures to multipath steering methods, the above packed picture has been sent to the single way and now we upgraded with the multipath directing calculation, at last we get an effective transmission and dependable, productive picture. They present three vital systems in particular cryptography, multipath steering calculation as well as steganography. The cryptography presents a novel plan for distinguishable reversible information concealing. The steganography approach for Least Significant Bit (LSB).And the multipath steering calculation includes in the dynamic nature of remote connections. These three procedures are consolidated together alongside the Huffman calculation, to encode the picture in a proficient way. The picture can be partitioned into six sections and which results in an alternate new image.

Manoj kumar and et al. (2013) [21] Digital data is transmitted utilizing Internet. Hence digital data should secure, copyright ensured, and confirmed in meantime. They proposed an algorithm to ensure digital data by implanting watermark that is encrypted using DES algorithm. Two level discrete wavelet Transformation (DWT) is connected to first picture. This guarantees power of proposed plan. DES encryption to watermark with key as well as repeating operations guarantee security of watermark data. Encryption as well as decryption key is same for both procedures. In event that we need to concentrate watermark picture, it is must to get secret key. Test result demonstrates that watermark is strong against different assaults.

Shahram Etemadi Borujeni et al. (2013) [2] had proposed a model that had encrypted in order to not recognize by others. As we know the image which is encrypted in frequency domain is very useful in digital and optical image processing whereas the time-domain encryption is limited to image communication. So in this paper we have given a hybrid approach that is using both chaotic image encryption in both time and frequency domain in order to encrypt the original image. Fridrich suggested a time domain chaotic image encryption. In tent map which is a function of chaotic is used to generate a random image which is further merged with the original image to get the encrypted image and all this is done on a frequency domain. Chaotic pixels substitution creates another encrypted image which is going to get merged in previously developed image .In this paper the image is also encrypted in time domain in non linear form and then is XORed with the image data. In this the chaotic phase magnitude will do the job in frequency domain whereas the 2dimensional Discrete Fourier Transform (DFT) will work in the plain image to change the domain of the image. In this it is also taken care that the key space analysis should be large in order to make the brute force attack infeasible.

Benyamin Norouzi et al. (2014) [16] had proposed a model which uses a 512 bit long key which is secret as the input value for the salsa20 hash function. In this first of all the hash function is changed and then generated a key which makes the encryption more secure. The encrypted text is created by correlating the key stream and the original text in order to create the encrypted message. As we know that the diffusion can crack the correlation of the values which are given and also change the pixel values. Then the image is encrypted again by using

2 rounds of diffusion. In the first round first of all the image is partitioned in the horizontal direction and in the second round of diffusion again same is performed but in the vertical direction to transpose the image which we get.

Iqtadar Hussain et al. (2014) [13] proposed a method for encryption of image is done by shuffling the pixel of image according to the chaotic technique. In which the all the pixels of image get combined using the tent map and then the plain image and cipher image get transformed using the S Box. They had used encryption algorithm on modified image using couple map latticed technique to do encryption. It uses tent map for chaotic which makes the image more secure. It uses transformation of s-box in order to encrypt the image. So in this paper firstly the image is get mixed up using the chaotic tent map and the get substituted by using S box.

K.Ganesan et al. (2014) [09] realized security of information is one of the critical issue which ought to be remembered .Therefore so as to do keep up security there are different chaotic techniques which utilizes look up tables to build the rate of encryption and unscrambling procedure. So here they utilized eight dimensional chaotic techniques in light of the fact that from the late/recent years a substantial number of other chaotic techniques were given which were confronting different issues like security issues and robustness. So with a specific end goal to evacuate such mistake/issues they utilized eight dimensional chaotic technique which uses look table which works as per the cipher block chaining. this technique does not utilizes XOR or XNOR as these are extremely delicate before known plain text assault. This encryption gives mass data capacity has more noteworthy repetition.

Snehal patil et al (2014) [19] did numerous security calculations that are utilized for security reason. Thought is one of them. The square figure IDEA works with 64-bit plaintext and figure content squares and is controlled by a 128-bit key. The major development in the configuration of this calculation is the utilization of operations from three distinctive mathematical gatherings. The calculation structure has been picked such that, with the special case that distinctive key sub-pieces are utilized, the encryption procedure is indistinguishable to the unscrambling methodology. The downside of thought is that the substantial quantities of powerless keys were found in IDEA (International Data Encryption Algorithm).

Additionally another assault on cycle 6 of IDEA has been recognized. This paper depicts the configuration and execution of global information encryption calculation (IDEA) convention, it works on 64 bit plaintext furthermore the span of the key has been expanded from 128 bits to 256 bits. This expanded key size will expand the unpredictability of the calculation. To build the measure of dispersion two MA pieces (multiplicative added substance square) are utilized as a part of a solitary round of IDEA when contrasted with one MA piece utilized already as a part of a solitary round likewise utilize the 12 rounds rather than 8 rounds. With these alterations in the proposed calculation will build the cryptographic quality. The proposed calculations expanded the cryptographic quality and take out the deficiency of the current International Data Encryption calculation (IDEA).The future extent of Enhanced IDEA calculation is that it can likewise be actualized in equipment utilizing VLSI innovation.

An Enhanced IDEA (International Data Encryption Algorithm) is an all around relevant piece encryption calculation, which allows the compelling security of transmitted and put away information against unapproved access by outsiders. The Upgraded IDEA (International Data Encryption Algorithm) is a solid piece figure. In spite of the fact that there are numerous operations included in the whole calculation, just three diverse of operations are included furthermore expanded adjusts in calculation expands the security of a calculation. The Enhanced IDEA (International Data Encryption Algorithm) takes out the frail keys issue of an IDEA (International Data Encryption Algorithm) by key planning of an IDEA (International Information Encryption Algorithm).With a key of 256 bits long, Enhanced IDEA is significantly more secure than the broadly known DES and unique IDEA. The proposed calculations expanded the cryptographic quality and wipe out the deficiency of the current International information Encryption calculation (IDEA).The future extent of S-IDEA calculation is that it can likewise be actualized in equipment utilizing VLSI innovation.

Xingyuan, Wang et al. (2014) [23] created various S-boxes is by using chaotic technique in order to encrypt the image in a more secure manner. In this the image is divided into four groups and then is substituted by S-box to smash the image in different direction. In order to remove the correlation of adjacent pixels, we have to keep in mind that while creating S

boxes each S-box is different from the previous one as the image produced after each round is different. Chaotic have good uses for sensitive dependence on initial conditions. In this the image is divided in various groups and the each group is treated with different S-box in order to create an encrypted image. We have to keep in mind that before creating the new S-box we need to change the initial stage of the image.

Chapter 3

PRESENT WORK

3.1 OBJECTIVE OF THE STUDY

The main objective is to produce the image more secure and to give the user a more protected image within less time. The image obtained after using this kind of method is more secure and only the authenticated user is going to get the image. We use DWT to reduce the computation time because DWT helps in doing the computations faster. Moreover IDEA is less time consuming than other algorithms. Hence IDEA is used here for encrypting the image. IDEA is used because the users want fast and secure data transmission. Therefore the main work has been done on processing time and security. Objectives of the proposed methodology are:

- To produce the image which is secure and to give the user a more protected image.
- Image obtained after using this kind of method is more secure only the authenticated user is going to get that image.
- We use various DWT with help of other chaotic techniques to make the transmission more protected.
- To avoid unauthenticated user from using the personal data of other user.

3.2 PROPOSED WORK

As it is known that with the evolution of many new communication applications, the customers or the users want high data rates i.e. users want the fast sending and receiving of data and secure transmission. That is why DWT is implemented here which helps in fast computation of the data so that less time is consumed in data processing.DWR is new concept which converts the data in the form of wavelets before transmission. Hence it is difficult for the intruder to grasp the data and misuse it. Therefore DWT helps in secure transmission of data and images. Here the thesis involves dividing the image, application of DWT, encryption by IDEA algorithm, inverse IDEA algorithm, inverse DWT and then

finally combination of different parts of the image. Here the security is further improved because image has been divided and encryption is done on the randomly selected parts of the image using chaotic cryptography. By randomly selection of parts of the image the computational delay will be reduced. Then the image will be transmitted parts by parts. Therefore, if intruder gets single part of the image, he will not be able to misuse it because he will not be having the entire image.

3.3 RESEARCH METHODOLOGY

IDEA is used to make our data encrypted. We want the data to be more secure and unauthorized person cannot access the data. So in order to protect data, cryptography provides two methods to secure our data using symmetric method and asymmetric method. In symmetric method same key is utilized for encryption and decryption and in asymmetric key method different keys are used for purpose of encryption and decryption. For this DWT has been implemented in order to make picture more secure.

The methodology involves six phases:

a) Division phase
b) DWT application
c) Encryption by IDEA algorithm
d) Decryption by inverse IDEA algorithm
e) Inverse DWT
f) Combination of the image.

The flow chart of the methodology is as follows:

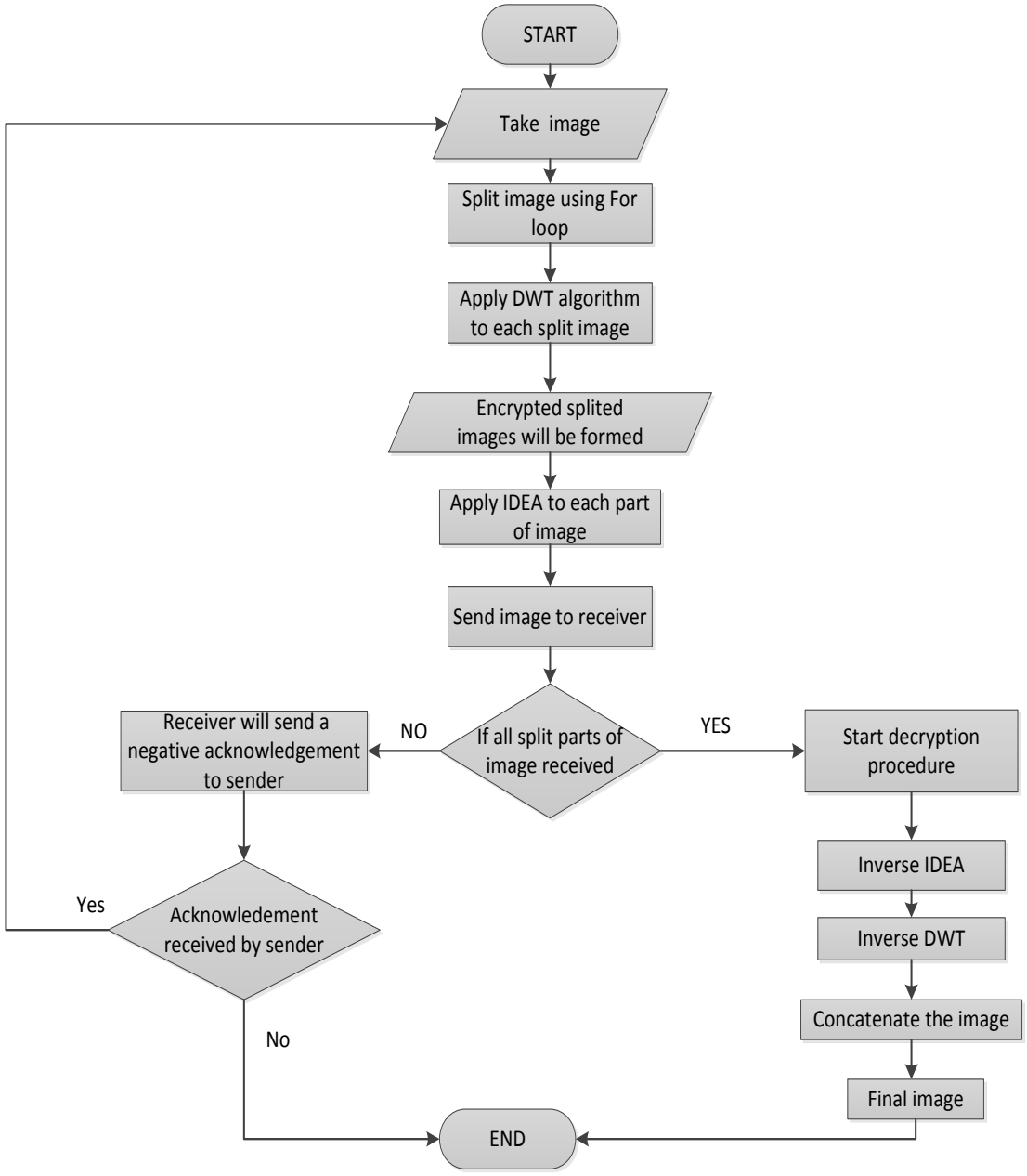

Fig. 3.3.1 Flowchart of Proposed methodology

Chapter 4

RESULTS AND DISCUSSIONS

When the data goes to the receiver after the encryption process, the receiver side undergoes decryption process. The image which was divided while encryption process is decrypted first which is shown in fig. 4.1. When all parts of the image are decrypted, all parts are combined together to form original image i.e plain text. The final original image is shown in fig 4.5.

Fig. 4.1 Divided images

Fig. 4.2 Decrypted and splitted image

Processing time has been reduced.

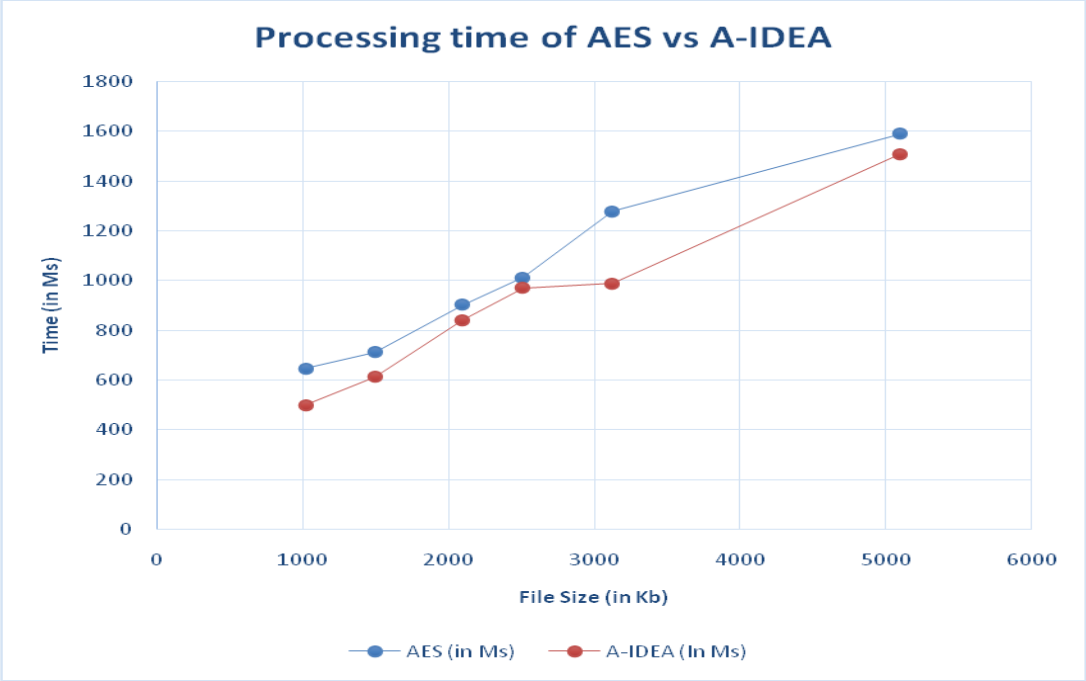

Fig 4.3 Graph of original and proposed work

Correlation Coefficient

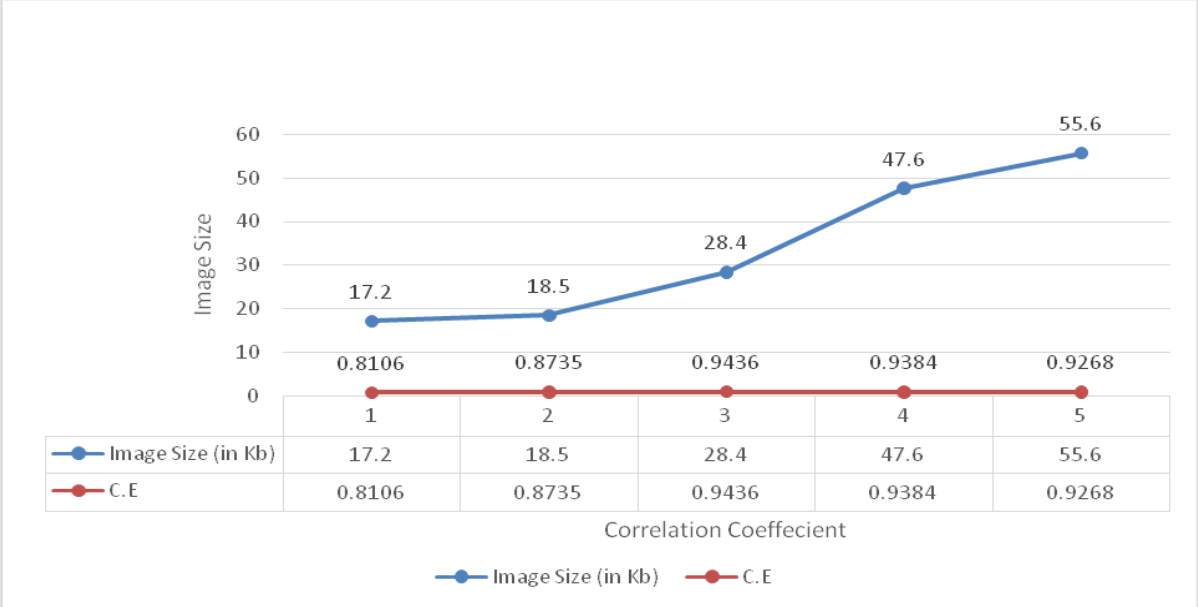

Fig 4.4 Graph of Correlation Coefficient

Fig. 4.5 Final decrypted image

Chapter 5

CONCLUSION AND FUTURE SCOPE

DWT is faster system than the Fast Fourier Transformation utilized before. Thus results will be conveyed sooner. In addition division of the picture upgraded the security in light of the fact that it will be troublesome for intruder to abuse the some piece of the picture. Along these lines sending picture to the next host will be faster as well as more secure. Further security is upgraded by IDEA calculation in light of the fact that IDEA is utilized for encryption which makes it troublesome for the intruder to comprehend the picture due to reason that DWT and encryption by IDEA has changed over the picture into the structure which is hard to get it. Besides IDEA will be connected to some randomly chosen parts of the picture thus computational as well as processing delay will be less.

Chapter 6

REFERENCES

[1] Abdullah, Abdul Hanan, Rasul Enayatifar, and Malrey Lee. "A hybrid genetic algorithm and chaotic function model for image encryption." *AEU-International Journal of Electronics and Communications* 66, no. 10 (2012): 806-816.

[2] Borujeni, Shahram Etemadi, and Mohammad Eshghi. "Chaotic image encryption system using phase-magnitude transformation and pixel substitution." *Telecommunication Systems* 52, no. 2 (2013): 525-537.

[3] Basu, Sandipan. "International Data Encryption Algorithm (Idea)–A Typical Illustration." *Journal of global research in Computer Science* 2, no. 7 (2011): 116-118.

[4] Castro, Julio Cesar Hernandez, José María Sierra, Andre Seznec, Antonio Izquierdo, and Arturo Ribagorda. "The strict avalanche criterion randomness test." *Mathematics and Computers in Simulation* 68, no. 1 (2005): 1-7.

[5] Daemen, Joan, and Craig Clapp. "Fast hashing and stream Encryption with PANAMA."In *Fast Software Encryption*, pp. 60-74. Springer Berlin Heidelberg.

[6] Dinghui, Zhang, Gu Qiujie, Pan Yonghua, and Zhang Xinghua. "Discrete chaotic encryption and decryption of digital images." In *Computer Science and Software Engineering, 2008 International Conference on*, vol. 3, pp. 849-852. IEEE, 2008.

[7] Dworkin, Morris. "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices." *NIST Special Publication* (2010).

[8] Engel, Dominik, Thomas Stütz, and Andreas Uhl. "Assessing JPEG2000 encryption with key-dependent wavelet packets." *EURASIP Journal on Information Security* 2012, no. 1 (2012): 1-16.

[9] Ganesan, K., and K. Murali. "Image encryption using eight dimensional chaotic cat map." *The European Physical Journal Special Topics* 223, no. 8 (2014): 1611-1622.

[10] Gupta, Dipalee, and Siddhartha Choubey. "Discrete Wavelet Transform for Image Processing." *International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001: 2008 Certified Journal, Volume 4, Issue 3*.

[11] Hermassi, Houcemeddine, Rhouma Rhouma, and Safya Belghith. "Improvement of an image encryption algorithm based on hyper-chaos." *Telecommunication Systems* 52, no. 2 (2013): 539-549.

[12] Huang, C. K., Chin-Wen Liao, S. L. Hsu, and Y. C. Jeng. "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system." *Telecommunication Systems* 52, no. 2 (2013): 563-571.

[13] Hussain, Iqtadar, and Muhammad Asif Gondal. "An extended image encryption using chaotic coupled map and S-box transformation." *Nonlinear Dynamics* 76, no. 2 (2014): 1355-1363.

[14] John Justin, M., and S. Manimurugan. "A Survey on Various Encryption Techniques." *International Journal of Soft Computing and Engineering (IJSCE) ISSN* 2231 (2012): 2307.

[15] Mahajan, Gaurav, and Kavita Upadhyay. "Performance Analysis of IDEA Encryption Model under Different Fading Environments."

[16] Norouzi, Benyamin, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, and Mohammad Reza Mosavi. "A novel image encryption based on hash function with only two-round diffusion process." *Multimedia Systems* 20, no. 1 (2014): 45-64.

[17] Osvik, Dag Arne, Joppe W. Bos, Deian Stefan, and David Canright. "Fast software AES encryption." In *Fast Software Encryption*, pp. 75-93. Springer Berlin Heidelberg, 2010.

[18] Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud. "Image encryption using chaotic logistic map." *Image and Vision Computing* 24, no. 9 (2006): 926-934.

[19] Patil, Ms Snehal. "An Enhancement In International Data Encryption Algorithm For Increasing Security."

[20] Sifuzzaman, M., M. R. Islam, and M. Z. Ali. "Application of wavelet transform and its advantages compared to Fourier transform." (2009).

[21] Tiwari, Nirupma, M. Kumar Ramaiya, and Monika Sharma. "Digital Watermarking using DWT and DES." In *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, pp. 1100-1102. IEEE, 2013.

[22] Vijayvargiya, Gaurav, Sanjay Silakari, and Rajeev Pandey. "A Survey: Various Techniques of Image Compression." *arXiv preprint arXiv:1311.6877* (2013).

[23] Wang, Xingyuan, and Qian Wang. "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos." *Nonlinear Dynamics* 75, no. 3 (2014): 567-576.

[24] Wei-bin, Chen, and Zhang Xin. "Image encryption algorithm based on Henon chaotic system." In *Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on*, pp. 94-97. IEEE, 2009.

[25] Zeghid, Medien, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. "A Modified AES Based Algorithm for Image Encryption." *International Journal of Computer Science & Engineering* 1, no. 1 (2007).

[26] http://en.wikipedia.org/wiki/Discrete_wavelet_transform

[27] http://en.wikipedia.org/wiki/List_of_chaotic_maps

[28]https://www.google.co.in/search?q=encryption+and+decryption&biw=1043&bih=504&source=lnms&tbm=isch&sa=X&ei=8L1JVezVINOcugSwxIGwDw&sqi=2&ved=0CAYQ_AUoAQ#imgrc=PPbHeCaXSeWV_M%253A%3ByjvyNuazUbuOBM%3Bhttp%253A%252F%252Fwww.sharonencyclo.com%252Fwp-content%252Fuploads%252F2015%252F03%252Fanu21.gif%3Bhttp%253A%252F%252Fwww.sharonencyclo.com%252Fcryptography%252F%3B666%3B336

[29] http://docs.oracle.com/cd/B19306_01/network.102/b14266/apdvncrp.htm#i1006212

[30] http://computer.howstuffworks.com/encryption.htm

[31] *https://users.cs.jmu.edu/.../IDEA-by-How-Shen-Chang-2004-FALL.doc*

[32] http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DWT	Discrete Wavelet Transformation
RSA	Ron River Adi Shamir and Leonardo Adleman
RAM	Random Access Memory
IDEA	International Data Encryption Algorithm

Encryption: Encryption is the transformation of electronic information into another structure/form, called cipher text, which can't be effortlessly seen by anybody with the exception of approved/authorized users.

Decryption: Decoding is the methodology of changing over scrambled information again into its original structure, so that it can be understood by the receiver. Encryption and unscrambling ought not to be misunderstood for encoding and interpreting/decoding, in which information is changed over from one structure onto another willingly.

Cryptographic attack: A cryptographic assault/attack is a system for bypassing the security of a cryptographic framework by discovering vulnerabilities in a code, figure, cryptographic convention or key administration plan. This methodology is additionally known as "cryptanalysis".

Cipher text: In case of cryptography, cipher text (or cyphertext) is consequence of scrambling/encryption executed on plaintext utilizing a calculation/algorithm, known as cipher.

Plain text: In cryptography, plain content alludes to any message that is not scrambled.

Public key: public key cryptography, otherwise called asymmetric cryptography, is a class of cryptographic conventions/protocols in view of calculations that oblige two different keys, one of which is mystery (or private) and one of which is open.

Private Key: a cryptographic key that can be got and utilized by anybody to encode messages planned for a specific beneficiary, such that the scrambled messages can be deciphered just by utilizing a second key that is known just to the beneficiary (the private key).

Cryptography: Cryptography is a system for putting away and transmitting information in a specific shape so that those for whom it is proposed can read and methodology it.
Cryptography is nearly identified with the orders of cryptology and cryptanalysis. Cryptography incorporates systems, for example, microdots, combining words with pictures, and different approaches to shroud data away or travel. Be that as it may, in today's PC driven world, cryptography is regularly connected with scrambling plaintext (standard content, infrequently alluded to as clear text) into cipher text (a procedure called encryption), then back once more (known as unscrambling). People who hone this field are known as cryptographers.

DWT: In numerical examination and useful investigation, a discrete wavelet Transform (DWT) is any wavelet change for which the wavelets are discretely tested/sampled. Likewise with other wavelet changes, a key playing point it has more advantage than Fourier transform because Fourier is transient determination/temporal resolution: it catches both frequency as well as location data (location in time).

IDEA: IDEA scrambles a 64-bit piece of plaintext to 64-bit block of cipher text. It employs a 128-bit key. The calculation comprises of eight indistinguishable rounds and a "half" round last change.

Chaos theory: Chaos Theory is a scientific sub-teaches that studies complex frameworks. Samples of these complex frameworks are many. Chaos Theory helped in randomly choosing values from given set of data. it helps in image encryption to select some parts of the image randomly using some generators to do encryption.

Random numbers: random numbers are helpful for a mixed bag of purposes, for example, creating information encryption keys, reproducing and displaying complex phenomena and for selecting irregular specimens from bigger information sets. They have likewise been utilized stylishly, for instance in writing and music, and are obviously ever prevalent for amusements and betting. At the point when examining single numbers, an arbitrary number

is one that is drawn from a situated of conceivable qualities, each of which is similarly plausible, i.e., a uniform dissemination. At the point when talking about a grouping of arbitrary numbers, every number drawn must be factually autonomous of the others.

Pseudo random number generators: As "pseudo" proposes, pseudo-irregular numbers are not arbitrary in the way you may expect, at any rate not in case you're utilized to dice rolls or lottery tickets. Basically, PRNGs are calculations that utilization numerical formulae or essentially precalculated tables to deliver arrangements of numbers that seem arbitrary. A decent sample of a PRNG is the straight congruential system. A decent arrangement of exploration has gone into pseudo-irregular number hypothesis, and present day calculations for creating pseudo-arbitrary numbers are good to the point that the numbers look precisely like they were truly irregular.