International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-5, August-2020
www.ijprse.com

Multilevel Image Encryption and Decryption Based On Biometric Approach

Kavya Ravishankar[1], Poornima Badgi[2], Neha K S[2], Nandini[2]

[1]*Assistant Professor, Department of Computer Science, Maharaja Institute of Technology Mysore, Visvesvaraya Technological University, India.*

[2]*Student, Department of Computer Science, Maharaja Institute of Technology Mysore, Visvesvaraya Technological University, India.*

Corresponding Author: poornimabadgib@gmail.com

Abstract: The field of Encryption is getting popularity in the current period in which information security is of utmost concern. Security is a noteworthy issue in correspondence to pictures; Encryption is one of the ways to deal with security. Picture encryption has application in web correspondence, intelligent media structure, clinical imaging, telemedicine, military correspondence, etc. Picture is not quite the same as text when it comes to encryption. In spite of the fact that we may utilize the customary cryptosystems to encode pictures legitimately, it's anything but a smart thought for two reasons. First is that the picture size is quite often a lot more noteworthy. Secondly, the conventional cryptosystems need a lot of time to straightforwardly scramble the picture information. The other issue is that the decoded text must be equivalent to the first content. Be that as it may, this prerequisite a bit much for picture information. Because of the attribute of human observation, a decoded picture containing little twisting is generally satisfactory.

Key Words: - ***Image Encryption, Pixel value based rotation, Block Shifting, Security of Image.***

I. INTRODUCTION

With the quick movement of information trade in electronic manner, data security is getting more significant in information stockpiling and transmission. Due to broadly utilization of picture in modern procedure, it is essential to shield the private picture information from unapproved get to. So encryption is utilized to safely communicate information in open systems. Each kind of information has its own highlights, therefore various procedures ought to be utilized to shield image data from unauthorized access. The majority of accessible encryption calculations are for the most part utilized for literary information and may not be reasonable for interactive media information, for example, pictures. In this structure we have introduced a square assembled change estimations dependent on the pixel regard transformation of picture. The amount of pixel upset relies upon the discretionary number.

II. LITERATURE SURVEY

Manju Kumari et.al carried out a work on Survey of Image Encryption Algorithms [1] in which they have proposed, security of information or pictures is one of the critical angles in the immense and as yet extending area of advanced exchange. Encryption of pictures is one of the notable instruments to protect privacy of pictures over a solid unlimited open media. This medium is vulnerable to assaults and thus proficient encryption calculations are need for secure information transfer. Various Strategies are proposed in writing till date, each have an edge over the other to make up for lost time to the regularly developing need of security. This paper is a push to dissect the standard techniques which are open dependent on various shows estimations like differential, verifiable and quantitative attacks examination. To check viability, all the forefront and grown-up methodology are executed in MATLAB-2015.

Suchita Tayde et.al carried out a work on “File Encryption and Decryption using AES Algorithm in Android phone” [2] in which they have proposed that today cell phones are generally significant and constant thing for every individual. In view of growing usage of cutting edge cell phone, tablet, PC, advancement of web, sight and sound development in our overall population mechanized picture and information security is the most fundamental issue. Criminal or crook is a dull individual who analyzes and changes the data while transmission happens. So to ensure such touchy information has become request of the day. Encryption is one of the strategy which is utilized to shield the delicate information from the unapproved individual. There are two sorts of encryption figuring Symmetric keys encryption and Asymmetric keys encryption. Just one key is utilized to scramble and interpret information. Key ought to be appropriated before transmission between substances. Keys anticipate vital occupation. Assorted symmetric key encryption calculations are DES, AES and Blowfish algorithms. In Asymmetric key encryption or open key encryption, two keys are utilized, they are private and open

key. Open key is utilized for encryption and private key for Decryption. Since customer will as a rule use two keys, Public key which is known to be open and private key known to user. (E.g. RSA and Digital Signatures). There is no prerequisite for flowing them going before transmission.

Savitri. G et.al carried out a work on Android Application for Secret Image transmission and Reception Using chaotic Steganography [3] in which they have proposed, Data covering up is a workmanship which has been utilized since long back for convert correspondence. Steganography is the specialty of concealing mystery message inside a bigger picture or a mystery picture in another spread picture, with the end goal that the shrouded message or a picture is imperceptible. Riotous frameworks are known for its arbitrariness; it very well may be made used in accomplishing the encryption. In this paper tumult based encryption calculation for pictures is utilized. This calculation depends on pixel scrambling where in the irregularity of the confusion is made used to scramble the situation of the pixels. Irregular pixel addition technique is utilized for concealing the mystery picture in spread picture. This application is created utilizing the java programming language in Android Software Development pack. This application made for the Android working framework can be utilized in savvy cell phones for sending any picture in an emit way by concealing it in another bigger picture.

Ankit Gupta et.al have carried out a work on an Image Encryption using Block based Transformation and Bit Rotation Technique [4] in which they have proposed that Alongside the fast expanding development of PC and system advancements, pictures are being communicated increasingly more regularly. Security of picture is a major issue. Picture Information is exuberant and visual, and has been significant methods for communicating data of individual. There is numerous encryption calculation had been accessible every one having some quality and shortcoming. In this paper encryption strategy that joins the idea of square based change and pixel control is presented. The proposed strategies comprise of two phases: In first step we apply block based matrix transformation for pixel position manipulation. In second stage, apply bit rotation technique that change the value of each pixel.

Mohammad Ali BaniYounes et.al carried work on Image Encryption Using Block-Based Transformation Algorithm [5] In which they have proposed also, principles for the encryption of information, advanced pictures and MPEG video. The overall model an average encryption/decoding framework about the security rule is talked about. Information encryption principally is the scrambling of the substance of information, text, picture, sound, and video and to make the make the information mixed up, undetectable or endless during figure text transmission. The objective is to secure the substance of the information against the aggressors. The opposite of information encryption is information Decryption, which recoups the first information. There are two kinds of encryption/unscrambling key: the open key framework and private framework. The most encouraging highlights are joint lossless pressure, joint encryption and concealing dependent on SCAN language which investigations the extraordinary properties of computerized picture and video and quest for high security calculations to lessen the general computational expense.

M Yang et.al worked on Data Image Video Encryption [6] in which they have proposed the most representative algorithm what's more, principles for the encryption of information, advanced pictures and MPEG video. The overall model a run of the mill encryption/unscrambling framework about the security standard is examined. Information encryption for the most part is the scrambling of the substance of information, text, picture, sound, and video and to make the make the information mixed up, undetectable or immeasurable during figure text transmission. The objective is to ensure the substance of the information against the aggressors. There are two sorts of encryption/decoding key: the open key framework and private framework. The most encouraging highlights are joint lossless pressure, joint encryption and concealing dependent on SCAN language which examinations the interesting properties of computerized picture and video and quest for high security calculations to lessen the computational expense

III. SYSTEM ARCHITECTURE

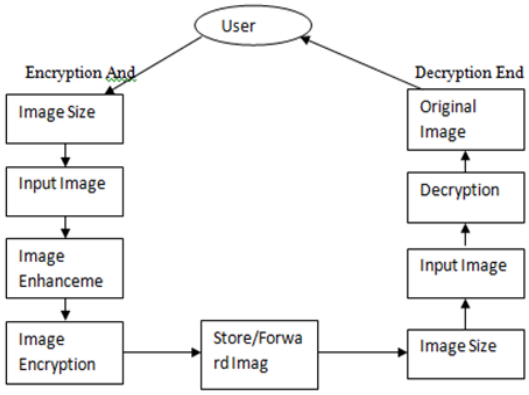

Fig.1: Overall system Architecture

International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-5, August-2020
www.ijprse.com

As the aim of this work is to enhance quality of the image and also provide a good image encryption algorithm. The above system architecture explains the steps of operation during Image Enhancement, Encryption and Decryption Here the user knowledge of operating the system plays an important role.

Highlights:

The fundamental target of this venture is to build up an improved picture encryption calculation utilizing pixel esteem turn.

- Encryption utilizing pixel esteem turn is a basic and significant method.
- In this technique utilizing key worth is extremely straightforward scientific activity which consumes less cup memory and the execution time is additionally exceptionally quick contrasted with existing strategy.
- Encryption of picture utilizing pixel esteem turn dependent on key worth is a misfortune less pressure.
- Image encryption has wide scope of utilization in clinical imaging, web correspondence and in guard correspondence and so on.
- So utilizing this sort of encryption technique gives a lossless pressure and it gives a safe and accurate picture.

IV. Proposed Work

A. Encryption

The goal of Twofold Encryption strategy is to handle the security issues while putting away and communicating pictures. In the main stage, Fingerprint of the client is considered as security key and Biometric esteem is utilized for making picture "square moving" and number of pixel esteem revolutions.

B. Decryption

To get back the first picture, twofold Decoding is applied. It is the technique opposite to Encryption. If the Fingerprint of user is coordinated, at that point pixel worth based Pivot calculation is applied. And second period of Unscrambling utilizes Square Moving. In this step the picture is partitioned into 8 squares and is rearranged. In the third stage, pixel worth based Turn estimation is used. Here, estimation of each pixel of each square is turned, considering the absolute of number estimations of key entered by the customer.

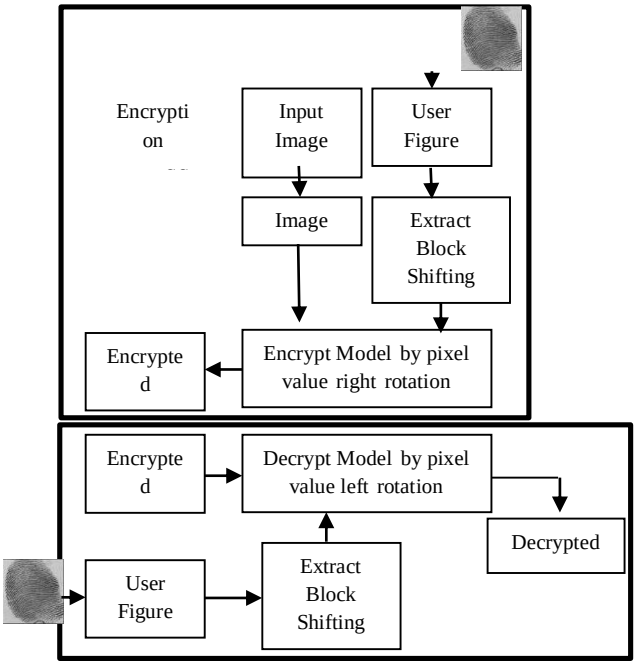

Fig.2. Block diagram of the proposed approach

V. Working Procedure

A. Encryption

The goal of twofold Encryption philosophy is to tackle the security issues while dealing with pictures. In the main stage, Fingerprint of user is utilized as security key. Fingerprint values are utilized for making picture "square moving" and number of pixel respect changes. In the ensuing stage "block shifting" estimations are done. Here, the picture is distributed into 8 squares and are improved.

In the third stage, “pixel value based rotation” calculation is utilized. Here, estimation of every pixel of each square is turned in view of the aggregate of whole number estimations of key entered by the client.

B. Decryption

To get back the first picture, twofold Decryption is applied which is converse procedure of Encryption. On the off chance that the Biometric is coordinated, at that point pixel value based rotation calculations are applied What's more, second period of decryption utilizes block shifting procedure will be performed.

International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-5, August-2020
www.ijprse.com

Dividing into blocks:

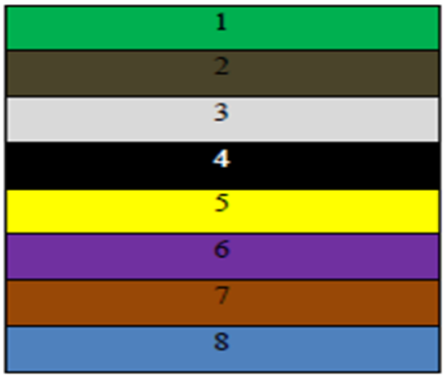

Fig.2: Depicts that the image is divided into 8 blocks
This is the first phase of encryption process.

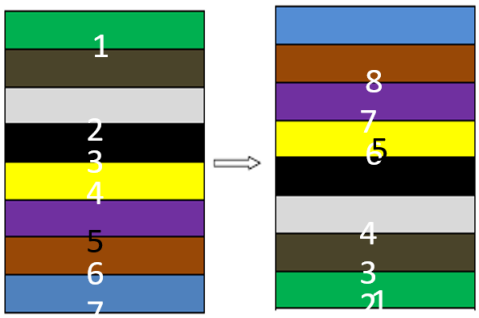

Fig.3: Depicts that the blocks in image are shuffled using "block shifting" algorithm. This is the 2nd phase of Decryption.

Encrypt Each Block:

Fig.4. Delineates the 2nd period of Encryption, pixel value based rotation" algorithm is applied by assigning each bit of sum to each block, each pixel value of every block is left rotated.

C. Module Description

This project consists of two main modules they are,

- Enhancement module
- Encryption module
- Decryption module

Enhancement Module:

Every one expect the image to be of fine quality, therefore the quality of image is checked supported many factors like intensity of pixel, distribution of pixel. And its entropy value etc. therefore the bad quality of image needs to be enhanced hence the strategy the histogram equalization is employed to boost the standard of image. Below diagram shows represents enhancement Module.

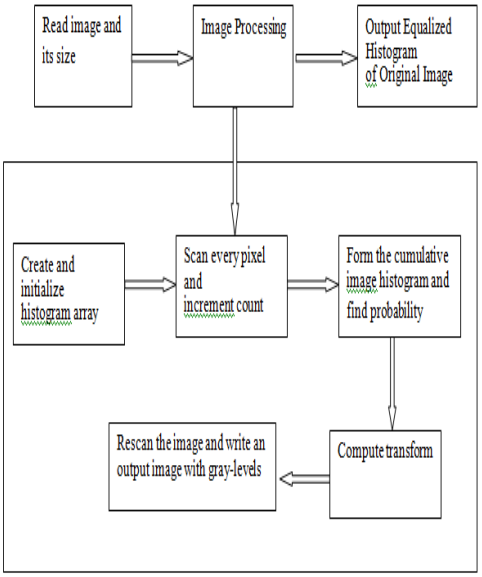

Fig.5. Block Diagram of Enhancement Module

Encryption Module:

Encryption is the way toward changing over picture starting with one from that point onto the next from which is difficult to reach to unapproved clients, so encryption which is utilizing pixel esteem pivot dependent on key worth fills in as an effective strategy.

International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-5, August-2020
www.ijprse.com

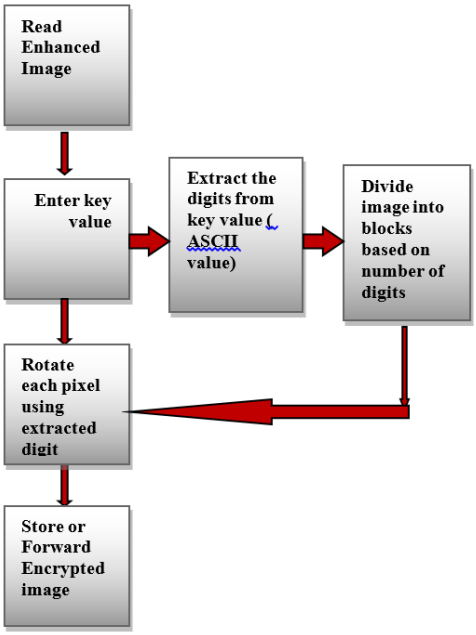

Fig.6: Block Diagram of Encryption Module

Decryption Module:

Decryption is the opposite procedure of encryption where the first picture is recovered by entering the correct key worth. The proposed method is a productive strategy at decoding end precisely an improved unique picture is recovered.

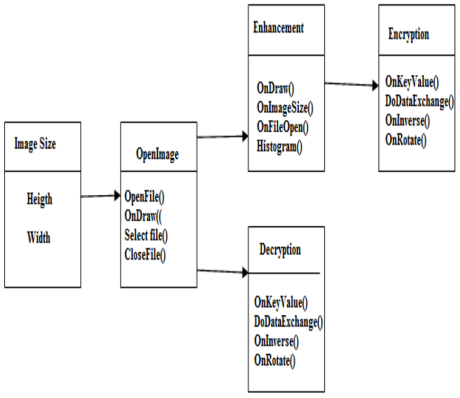

Fig.7. Class diagram

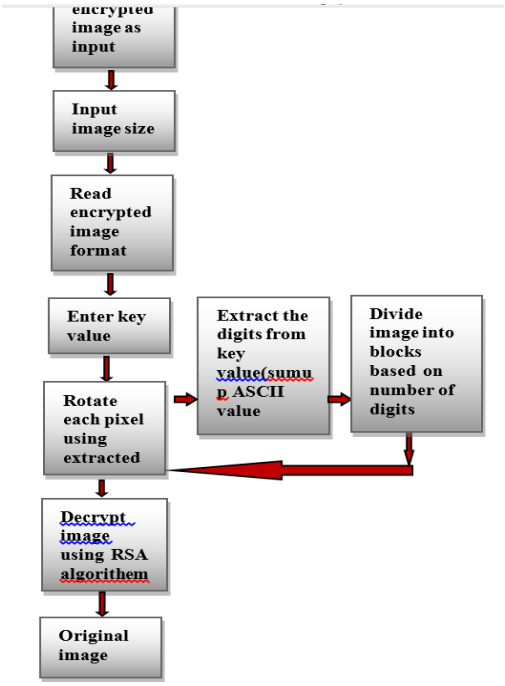

Fig.8: Block Diagram for Decryption Module

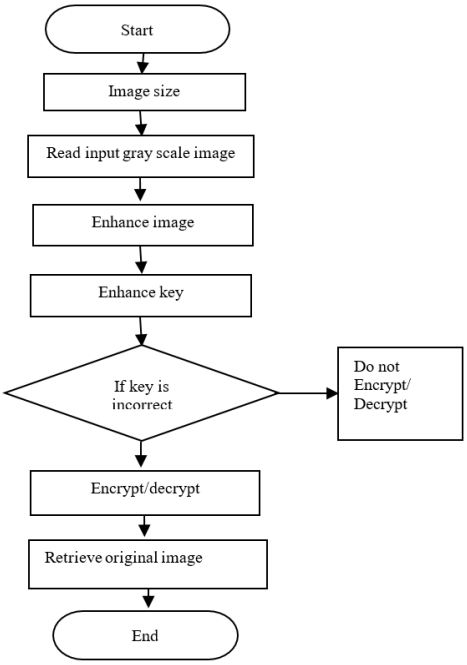

Fig.9. Data flow diagram for proposed system

VI. Conclusion And Future Scope

The Project gives a generally excellent improved encryption calculation for picture encryption, Where the calculation utilizes a key as an incentive to isolate and turn the pixels, which is only a basic numerical activity, devours less CPU memory and lessens the execution time. It utilizes a basic RSA calculation whose effectiveness in bit activity is more. Since it is a lossless pressure client gets definite Unique picture. The nature of the picture is additionally improved by doing the procedure of histogram evening out with the goal that client at beneficiary end gets a definite and upgraded unique picture.

Future Work:

This calculation can be actualized in other platforms like Android java and so forth. This method can be utilized to make sure about other mixed media information like Video Transfer. Image quality can be improved utilizing a wide range of sorts of histogram adjustment. Can additionally be utilized to make sure about picture information in versatile applications. This Algorithm can likewise be utilized to scramble video arrangement.

References

[1]. Manju Kumari, Shailender Gupta, Pranshul Sardana, "A Survey of Image Encryption Algorithms", 3DR Review First Online: 13 November 2017

[2]. Suchita Tayde, Asst Prof. Seema Silender, "File Encryption, Decryption Using AES Algorithm in Android phone ",2015.

[3]. Savithri G, K.L.Sudha, "Android Application for Secret Image transmission and Reception Using Chaotic Steganography",2014 .

[4]. Ankit Gupta, Namita Tiwari, Meenu Chawla, Madhu Shandilya, "An Image Encryption using Block based Transformation and Bit Rotation Technique ", 2014.

[5]. Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm",2008.

[6]. M. Yang, N. Bourbakis, and S. Li, "Data-image video Encryption," potential, IEEE, vol. 23, no. 3, pp. 28-34, 2004.

[7]. Honnaraju B, Manoj Kumar M, Shiva Sumanth Reddy, "Image Encryption by using Pixel Value Rotation",2012.

[8]. S. Li, C. Li, G. Chen, N. G. BourBakis, and K.-T. Lo, "A General quantitative cryptanalysis of Permutation-only Multimedia ciphers against plaintext attacks," Signal Processing: Image Communication, vol. 23, no. 3, pp.212-223, 2008.

[9]. K. C. lyer and A. Subramanya, "Image Encryption by Pixel Property Separation," http://eprint.iacr.org/2009/043.pdf, Cryptology ePrint Archive, 2009.

[10]. "Implementing a simple histogram equalisation algorithm in Reconfigurable Hardware" Stephanie Parker.

[11]. Rafael C. Gonzalez University of Tennessee, Richard E. Woods Med Data Interactive Upper, a Book on "Digital image processing "Third edition, 2008 by Pearson Education, Pearson Prentice Hall Pearson Education, Inc. Upper Saddle River, New Jersey 07458.

[12]. Ratinder Kaur, V. K. Banga "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) July 15-16, 2012.

[13]. Yaobin Mao1 and Guanrong Chen2 "Chaos-Based Image Encryption" Nanjing University of Science and Technology.

[14]. Jawad Ahmad and Farad Ahmed" Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04 18.