Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 6, August-2018, ISSN 2230-7540

Mobile Image Vision and Image Processing Reliability Design for Fault Free Tolerance in Traffic Jam

Priyanka Kaushik[1]* Dr. Rajeev Yadav[2]

[1] Research Scholar, Computer Science and Engineering Department

[2] Professor, OPJS University Churu, Rajasthan, India

Abstract – Image vision has been studied by many perspectives. It not only important study of graphics but use in multidisciplinary fields. it provide reliability and less chance of hacking or theft while transferring or transporting the data and moreover if we decrypt it and then zip it or break and fuse the original image into various pixel then it will maintain the data transfer speed and avoid the traffic jam situation and fusion of data provide the reliability and safety of the data. it expands from raw data recording into techniques and ideas combining digital image processing, pattern recognition, machine learning and computer graphics and mobile computing especially it is useful for the data safety while transferring the data in traffic jam it minimize the chances of image and data lost during the congestion and articulation point in traffic jam .

Key Words – Pattern Recognition, Decryption, Sharing-Resources, Cipher-Image.

----------X----------

1. INTRODUCTION

Security for Radio Frequency Identification (RFID) devices has received expanding consideration in the course of recent years. This is mostly because of security issues, which may hamper the acknowledgment of RFID technology. A moment reason is the materialness of RFID innovation for item validation.

It not only important study of graphics but use in multidisciplinary fields. it provide reliability and less chance of hacking or theft while transferring or transporting the data and moreover if we decrypt it and then zip it or break and fuse the original image into various pixel then it will maintain the data transfer speed and avoid the traffic jam situation and fusion of data provide the reliability and safety of the data.

Product piracy, the creation and offering of fake items, regularly utilizing the production network of the genuine producer, is a monetarily important issue. The misfortunes incurred about by it effectively accomplish the multi-billion range [LLMF07]. Item confirmation can possibly at any rate ease, if not totally stop, item theft. RFID innovation is now utilized in production network administration as a trade for the scanner tag recognizable proof framework. On the off chance that it could be empowered with confirmation abilities this would be an incredible leap forward. Security in data frameworks has dependably been connected with cryptography. The work of sound cryptographic primitives is troublesome for a security application.

Elliptic Curve Cryptography (ECC) is the most resource traditionalist open key cryptosystem as of now known. The serious conditions involved by a encryption domain make ECC the main feasible answer for sound cryptography for image ciphering. The security of every ECC primitive, including verification, relies on the point augmentation operation.

This means to build up a point increase segment that could be conveyed on an image ciphering system. For this an approach novel to low power, little zone ECC plan for RFID applications was picked. Moreover uncommon care was taken to make the circuit strong against side channel assaults.

Elliptic curves are algebraic curves which have been considered by numerous mathematicians for a long time. In 1985, Neal (Koblitz 1987) and Victor (Miller 1986) independently proposed the public key cryptosystems utilizing elliptic curve. From that point forward, numerous scientists have invested years concentrate the quality of ECC and enhancing systems for its usage. The Elliptic bend cryptosystem (ECC) gives a littler and quicker public key cryptosystem. Likewise, the ECC is additionally a

practical and secured innovation to be actualized in compelled applications

2. LITERATURE REVIEW

N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal,[1] The developing critical requirement for an ever increasing number of secure frameworks has driven specialists worldwide to find and execute more current methods for encryption. Public key cryptography systems are increasing overall ubiquity for their simplicity and better quality. With the fast improvements of the communication and uses of media strategies as of late lead the researchers to concentrates on the security of digital information over the web. This examination has talked about the utilization of Elliptical Curve Cryptography for ciphering shading pictures. ECC has been demonstrated to score over RSA on the premise of its quality and speed. This exploration utilized NIST Curves for ciphering colour image.

B. Aissa, D. Nadir and M. Ammar,[2] This treats the security of images. Managing the issue of image encryption and decryption. The encryption plan is finished by utilizing the stream cipher framework in light of the nonlinear mix generator. The proposed keystream generator comprises of fourteen binary primitive nonlinear input move registers (NLFSRs) and one Boolean capacity. The Boolean capacity consolidates the yield successions of the fourteen NLFSRs to deliver the keystream. All criticism move registers utilized in the keystream generator are primitive and nonlinear. The proposed encryption plan is basic and very productive. Security investigation covers key affectability examination, key space examination, connection coefficient investigation, clamor investigation, measurable attacks, Berlekamp-Massey attack, relationship attack and algebraic attack. In light of trial results and the security investigation it can be presumed that the proposed encryption plan is exceptionally key delicate, profoundly imperviousness to the commotions and demonstrates a decent resistance against animal constrain, measurable attacks, Berlekamp-Massey attack, relationship attack and algebraic attack.

Ranjith Kumar R. and Saranraj B.[3] In this research image encryption algorithm in light of confusion and diffusion utilizing dynamic key space is proposed. Confusion of pixels is finished by triangular confusion, strategy proposed in this work and diffusion is finished by values acquired from logistic map iterations. An inside key generator is utilized to generate the underlying seeds for the general encryption conspire proposed, with these underlying seeds, strategic guide produces pseudo arbitrary numbers which are then changed over into Confusion arrange (CO) for disarray. Perplexity request is connected to the squares which have experienced triangular disarray. The dispersion bits (DFB) are created in parallel utilizing the strategic guide and controlled with pixels befuddled by perplexity arranges. The image pixels are iteratively mistaken and diffused for CO and DFB separately to create cipher image in least number of rounds. This work concentrates on key era utilizing strategic and tent maps with iterative reproduction to secure the image. Disarray based technique gives a dynamic changes to perplexity and dispersion design in the image encryption. A single bit change in the key will drastically change the outcome in the inside key era structure proposed. The reproduction comes about affirm that the agreeable level security is accomplished in three rounds and the general encryption time is saved.

A. N. Borodzhieva and P. K. Manoilov,[4] The research portrays an algorithm and created MATLAB-based module with choices for intuitive e-learning for encryption/decryption of texts utilizing bifid ciphers. It will be utilized as a part of the course "Telecommunications Security", included as obligatory in the educational modules of the claim to fame "Telecommunication Systems" for Bachelor degree at the University of Ruse. The application permits choosing the dialect and the parameters of the encryption/decryption key through menus. It delineates well ordered the procedure of encryption/decryption of the plain-text/cipher-text entered by the client, utilizing bifid ciphers. The oddity is that the algorithm for encryption/decryption of texts in English utilizing bifid ciphers is altered to be utilized for texts in Bulgarian, Russian and Romanian. The module has a plausibility to show data on bifid ciphers and to represent the rule of its operation in a different graphical window.

R. U. Ginting and R. Y. Dillak,[5] Doing a digital image transmission over web require a safe security againts ilegall replicating. Shockingly, numerous present information encryption techniques, for example, DES, RSA, AES, and other appropriate for test information, yet not for digital image. This exploration propose new secure algorithm for image encryption, which in view of RC4 stream cipher algorithm and confused coordinations delineate. The proposed algorithm acts as takes after: (i0 changing over the outside key into starting quality, (ii) utilizing he beginning an incentive to create a key stream utilizing disordered calculated guide capacity, and (iii) preparing a stage and the outcome is then XOR-ed with bytes stream of digital image. The investigation comes about demonstrate that the proposed algorithm (i) can make the cipher-image cannot be outwardly recognized, (ii) can wipe out the measurable connection between's the plain-image and cipher-image, (iii) is exceptionally touchy to little changes of key, and (iv) has no adjustment in image substance (lossless encryption) amid encryption and decryption handle which is shown by the hash esteem (MD5) of plain-image has a similar hash esteem (MD5) wth decoded image.

M. Savari, M. Montazerolzohour and Y. E. Thiam,[6] The main part of encryption algorithms is to protect devises from attack. Utilizing the best and more

effective algorithm for a gadget as indicated by its stockpiling and measure of information exchange is the most vital part. This exploration thinks about Elliptical Curve Cryptography algorithm (ECC) with RSA algorithm on a multipurpose keen card. There are three applications in our multipurpose brilliant card which is named wellbeing, credit and international ID card. ECC is contrasted and 160 piece key size and RSA with 1024 piece key size. The aftereffect of examination is depicted in the last segment.

Table 1.1 Table of Literature Review

SR. NO.	TITLE	AUTHORS	YEAR	APPROACH
1	Elliptic Curve Cryptography for Ciphering Images	N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal,	2015	Discussed the use of Elliptical Curve Cryptography for ciphering color images.
2	An approach using stream cipher algorithm for image encryption and decryption,	B. Aissa, D. Nadir and M. Ammar,	2014	The encryption scheme is done by using the stream cipher system
3	A novel chaotic color image encryption / decryption based on triangular confusion,	Ranjith Kumar R. and Saranraj B.,	2014	Image encryption algorithm based on confusion and diffusion using dynamic key space.
4	MATLAB-based module for encryption and decryption using bifid ciphers applied in cryptosystems,	A. N. Berodzhieva and P. K. Manoilov,	2014	Developed MATLAB-based module with options for interactive e-learning for encryption/decryption of texts using bifid ciphers
5	Digital color image encryption using RC4 stream cipher and chaotic logistic map,	R. U. Ginting and R. Y. Dillak,	2013	New secure algorithm for image encryption, which based on RC4 stream cipher algorithm and chaotic logistics map.
6	Comparison of ECC and RSA algorithm in multipurpose smart card application,	M. Savari, M. Montazerolzohour and Y. E. Thiam,	2012	compares Elliptical Curve Cryptography algorithm (ECC) with RSA algorithm on a multipurpose smart card

Computer vision works by using an algorithm and optical sensors to stimulate human visualization to automatically extract valuable information from an object[13]. Compared to conventional methods that take a long time and require sophisticated laboratory analysis, computer vision has been expanded into a branch of artificial intelligence (artificial intelligence) and simulated human visualization.

It also combined with lighting systems to facilitate image acquisition continued with image analysis. In more detail, the stages of image analysis are: 1) image formation, in which image of object is captured and stored in computer; 2) image preprocessing, whereby quality of image is improved to enhance the image detail; 3) image segmentation, in which the object image is identified and separated from the background, 4) image measurement, where several significant features are quantized, and 5) image interpretation, where the extracted images are then interpreted[14].

The recent development of image processing technology has provided the possibility to create a system to recognize a digital image.

Pattern Recognition as a branch of computer vision focused on the process of object identification through image transformation to get a better image quality and image interpretation. This process aims to extract information to make decisions based on images obtained from sensors [5]. In other words, computer vision seeks to build an intelligent machine to "see." Common frameworks used in computer vision are image acquisition, pre-processing, feature extraction, detection/segmentation, high-level processing, and decision-making [5] , [6]. The computer vision frameworks consisted two main groups, e.g., 3D morphological analysis and pixel optimization. The 3D morphological review has been a standard theory for computer image processing and pattern recognition, whereas pixel optimization is related to characterization of pixel morphology, including structural analysis and internal components for a better understanding of vector function [32]. Also, the approach should be performed on relatively large data sets covering many layers of geometrical composition. Therefore, efficient and accurate computing algorithms to extract the relevant quantitative information are important to understand the complex color clusters as a whole. The integration of morphological analysis with some artificial intelligence methods can result in better performance through computing algorithms. The computing algorithm is fuzzy logic[33], artificial neural networks[34], and genetic algorithms[35]. They can be combined to completely complete complex tasks.

Table 1.2. Related research on computer vision

No	Name	Goals	Method	Results
1	Su, et al.,[28]	Estimation of solid depth map of a single monocular natural image	Bayesian methods to restore 3D scene structures	Superior performance after minimization of pixel-wise depth errors with training dataset but lower performance for objects taken from natural image.
2	Liu, et al., [29]	Comparison of image quality with different retargeting methods quickly and reliably	Reverse order (top-down)	Good consistency using certain metrics
3	Anharjafari, et al., [31]	Image-based Illumination Inspired by Using Decomposition of Local Singular Value and Discrete Wavelet Transformation	Image illumination enhancement on color pixel correction	This technique is compared to the general standard histogram distribution (GHE) and local histogram equalization (LHE).

There are two approaches to the segmentation and decryption recapture of image data. Segmentation is basically to divide an image into areas that are not overlapping (overlapping) [36] through specific algorithms to estimate an area of the image. The city is a collection of pixels that have the same unique characteristics as color, gray level, texture, and others.

The area is retrieval region of images .In general, the image segmentation approach that is often used is the method of intensity, color approach, shape and pixel pattern approach [37]. In most computer vision applications, border detection and image segmentation are a very important in the object image recognition interpretation, analyses and observation.

3. PROPOSED TECHNIQUE

The cryptographic technique is being discussed in this work is explained here and the different parts of the proposed encryption system is explained below.

The working of system is also explained with the help of flow charts after block diagrams.

In below figure the proposed system is explained with main blocks where the system is divided among multiple security layers. The first block is to twisting of red, green and blues layers with different flipping operation this is parallel security in a single layer itself. Followed by blending of layers i.e. RGB layers are mixed each other to make it more difficult to recover. The third level is chaotic mapping are also performed over RGB layer with different frequencies which will further complicate the encryption algorithm for enhancement of security. In the end of this we will get the encrypted image which is most secured image ever.

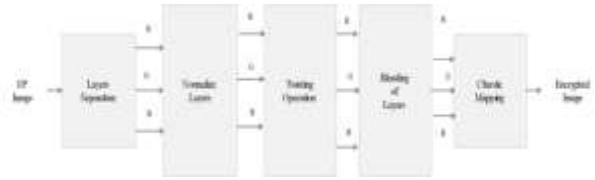

Figure 1.1 Basic Block Diagram of proposed system.

The decryption process is the reverse operation of encryption process and the steps are chaotic decryption of RGB layers with the specified frequencies followed by de-mixing of RGB layers and at the last reverse rotation of layers as it done on the angles.

The above system is implemented on image processing simulation tool and the flow of execution of algorithm is shown in below figures.

The flowchart of proposed Encryption and Decryption approach are given in the figure below.

Figure 1.2 Flow Chart of Encryption Process

A. Proposed Encryption

Select the image you want to use for the image ciphering purpose extract file for saving results read the selected image resize image to square shape and normalize layers of image and apply hybrid twisting on each layer blend the layers and apply chaotic image mapping with different frequencies. Save encrypted image and time required. Flow of the process has given in figure1.2.

B. Proposed Decryption

Figure1.3 demonstrated the flow of the proposed decryption system. To decrypt select the encrypted image which is to be decrypt. Decryption process is just a reverse of the encryption process. After selecting image apply reverse chaotic mapping and apply reverse blending of layers after reverse blending of layers reverse twisting of layers applied to image after that it shows decrypted image.

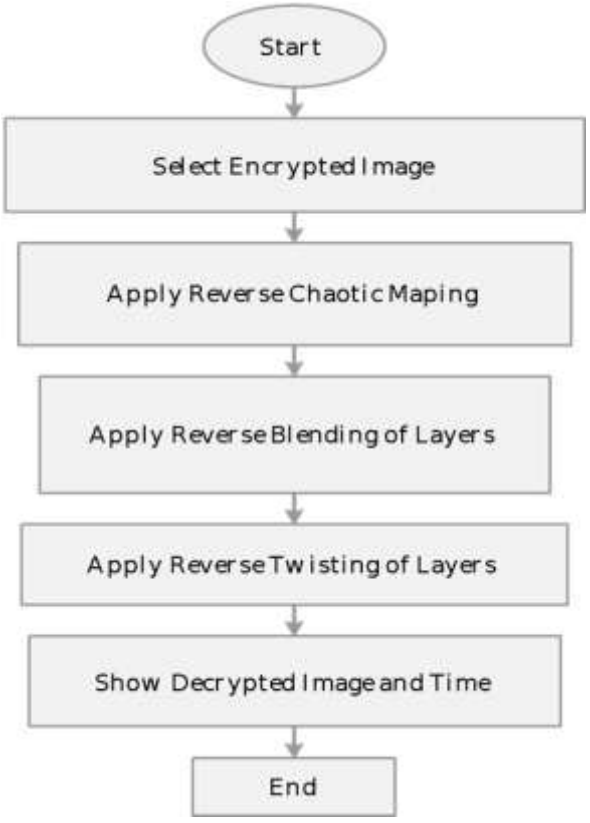

Figure 1.3 Flowchart of decryption process

Figure 1.4 Step 1: Input Images (Towar, lena, peppers and flinstone).

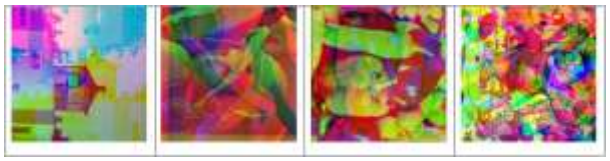

Figure 1.5 Step 2: Hybrid Twisting of Layers of Respective Previous Stage Outputs.

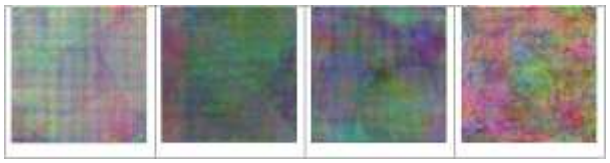

Figure 1.6 Step 3: Blending of Layers of Respective Previous Stage Outputs.

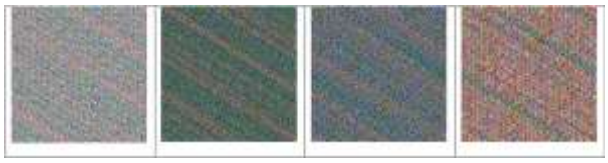

Fig1.7 Step 4: Chaotic Mapping Operations on Respective Previous Stage Outputs.

Table 1.1: Comparison of Encryption and Decryption Time.

Methodology	*Image Dimension in pixels*	*Encryption Time (sec.)*	*Decryption Time (sec.)*
Proposed	170x170	*0.09525*	*0.45533*
Existing [1]	170x170	0.575	10.161

Table 1.2: Individual Encryption and Decryption Timings in Seconds.

Image	*Image Dimension in pixels*	*Encryption Time (sec.)*	*Decryption Time (sec.)*
Tower (Base Paper)	*170x170*	*0.0952*	*0.4553*
Lena	*170x170*	*0.1047*	*0.4613*
Peppers	*170x170*	*0.0997*	*0.4549*
Flinstone	*170x170*	*0.0999*	*0.4452*

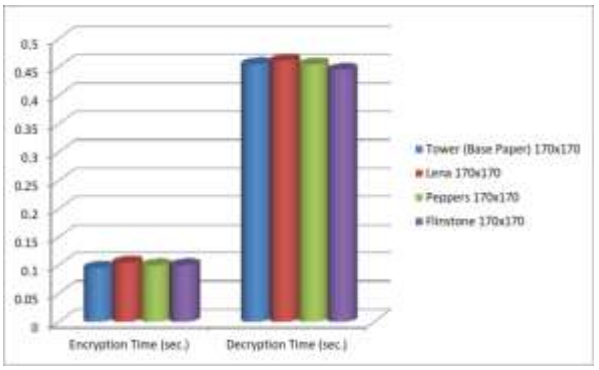

Fig.1.8 Graphical representation of individual encryption and decryption timings in Seconds

I. The table 2 shows the summary of images with respective Encryption and Decryption time and size of particular images where we can compare the size deference between images and encryption and decryption time which is in second.

II. The Table 1 shows the comparison of encryption and decryption time between proposed system and existing also.

4. CONCLUSION

A simulation is performed and the result of location updates through deployment of locators is achieved Simulation of cryptographic technique is worth implanting if it works faster when encrypting and decrypting also. The existing work has discussed about the image cryptography which was named elliptical curve method and has better encryption and decryption time. The challenge was to improve the speed i.e. reduction in encryption and decryption time. Existing methodology has 2 level of security to encrypt image and which was also need to maintain with taking into considerations that security levels must be increased to make the encryption more robust and crack free. This will make system and encrypted image is not even unreadable even untraceable, without the knowledge of security levels and algorithm. The encryption levels are here divided in parallel security also means all the layers RGB are not encrypted equally. This idea makes future encryption algorithms more secure even some of the old robust cryptography algorithms can modified with this concept to increase the shield of old systems and can facilitates the high end modern encryption systems. It expands from raw data recording into techniques and ideas combining digital image processing, pattern recognition, machine learning and computer graphics and mobile computing especially it is useful for the data safety while transferring the data in traffic jam it minimize the chances of image and data lost during the congestion and articulation point in traffic jam.

Computer vision has been related to image processing and machine learning. Computer vision

as a field of a wide array of discipline has been linked closely to image processing discipline. The Image processing, itself has brought benefits in different areas of technology especially to analyze images to obtain the necessary information. As technological areas to be developed with computer vision, it has been expanded to other engineering fields such as geographical remote sensing, robotics, computer and human communication, healthcare, and satellite communication. Researchers who interested in computer vision can use the knowledge to predict individual events by analyzing images and videos and extracting their features. As the developments in the field of computer vision are related closely to image processing and machine learning, it can be used to more extensive areas of studies to predict or detect object behavior and characteristics including human activities and natural events. Figure: (a) the object instance is changed to black and white; (b) Examples of objects of different size than their original size because of a scale factor; (c) Examples of objects being transparent or color combinations; (d) Examples of objects being black and white with scale arrangements and also changing positions differently from their real opinions. And in this manner if we decrypt image like this while transferring through various mobile protocols in mobile networking or during transferring the image packets through transport and network layer there will be less chance of congestion or articulation point in traffic jam which was previously due to large image data but it also provide reliability and fault tolerance free concept and environment.

5. REFERENCES

[1] N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal (2015). "Elliptic Curve Cryptography for ciphering images," 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, pp. 1-4.).

[2] B. Aissa, D. Nadir and M. Ammar (2014). "An approach using stream cipher algorithm for image encryption and decryption," 2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Hammamet, pp. 498-503.

[3] Ranjith Kumar R. and Saranraj B. (2014). "A novel chaotic color image encryption / decryption based on triangular confusion," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, pp. 94-100.

[4] A.N. Borodzhieva and P. K. Manoilov (2014). "MATLAB-based module for encryption and decryption using bifid ciphers applied in cryptosystems," 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME), Bucharest, pp. 287-291.

[5] R. U. Ginting and R. Y. Dillak (2013). "Digital color image encryption using RC4 stream cipher and chaotic logistic map," 2013 International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, pp. 101-105.

[6] M. Savari, M. Montazerolzohour and Y. E. Thiam (2012). "Comparison of ECC and RSA algorithm in multipurpose smart card application," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, pp. 49-53.

[7] Padma Bh, D. Chandravathi, P. Prapoorna Roja (2010). “Encoding and decoding Of a message in the implementation of Elliptic Curve Cryptography using Koblitz Method”. International Journal on Computer Science and Engineering (IJCSE) Vol. 02, No. 05, pp. 1904-1907

[8] Hankerson, Menezes, Vanstone (2004). “Guide to elliptic curve cryptography” Springer, 2004 ISBN 038795273X 332s_CsCr

[9] http://www.nsa.gov/business/programs/elliptic_curve.shtml

Corresponding Author

Priyanka Kaushik*

Research Scholar, Computer Science and Engineering Department