iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VIII **Month of publication:** August 2019

DOI: http://doi.org/10.22214/ijraset.2019.8130

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VIII, Aug 2019- Available at www.ijraset.com

Security of Cloud Data using Chaotic Mapping a Steganography

Hemalatha JK
Computer Science Engineering, M. Tech, VTU University Belagavi

Abstract: ***Data trade among sender and recipient turns out to be quick and simple. The nature of data operates like sending secret must be taken note. Hiding the data is necessary for securing information. It should be possible utilizing method like Cryptography and Steganography. In this framework the image steganography utilizing secret image and to hide secret image hence RGB image is used to cover. Encryption procedure is done to give a more dependable security. The picture is encrypted based on NCA principle to give more security for secret image we are applying modified a new efficient embedded algorithm using Embedded Least Significant Bits E-LSB. Steganography works space and for integrity checking. We first encrypt the data and then hide it in an image to fulfil our purpose.***
Keywords: Cryptography, Steganography, NCA, Embedded Least Significant Bits (E-LSB),

I. INTRODUCTION

Cloud storage is a web focused registering. It vivaciously conveys everything as an administration over the web dependent on client loads. For example, arrange framework stockpiling, equipment programming and assets. These administrations are characterized into three kinds as we known. Distributed computing is sorted out as three models, for example, Pub1ic, Private and Hybrid mists. Cloud data resides anywhere in the world moving to the public cloud or using hybrid. Cloud platform include Google, SAP, and Google drive etc. Along with the various advantages, new scheme is proposed for secure data storing technique considering the data integrity. After encrypt the data and then hide it in cover image, so that no one can detect the data from the stego image. And for integrity check there is no need for the third party for verification. In cryptography, using non linear chaotic algorithm for encryption and decryption, as in this case cryptography do not hide the information so steganography is introduced, new efficient embedding algorithm using E-LSB to hide the secret image or information this process gives the security of data. Integrity checking using hashing algorithm, information is encrypt and embed text message in a cover picture is used for least significant bits process all the pixels 8bits of Red R Green G and Blue B plane separately. This procedure is applied initially scramble the message and generating the hash code. Data is cover up, trusting that the encrypted image is decrypted using hash value and its message and NCA values are secret while fully completing the decryption. As NCA is a realistic encryption calculation which is secure enough, simply look at the steganography technique's security. In the wake of whacking data spread picture information location and information decimation are connected to esteem this framework. For example, jpeg pressure design transformation salt and pepper turn, during quality estimation we are showing signs of improvement PSNR worth, for example, in the wake of whacking in picture spread of pixels by get PSNR esteem and large around which is superior to the already existing strategies.

A. Importance Of Security

Security is the one which is of ensuring or protecting something like actually the information. Presently a day the security assumes an imperative part in day the today's world. It is becoming a more importance to give a secure each part of online information is to ensure system is secured. System security is assurance of access, abuse, and hacking of documents and registries in the computer framework. While sending information from one place to other place, security is used to protect that information.

1) *Cryptography:* The process of converting the original information text and vice-versa this process is called encryption. It is done by using public key and private key. At the receiver side authorized person to get original message it is called decryption. In cryptography, most important technology is key distribution. This technology is used to share key between the people key is known only sender and receiver. While sending information between the sender and receiver the hacker finds the key, then get information try to make some changes in information. Cryptography process can only encrypts and decrypts the information, but do not hide the information.
2) *Steganography:* Steganography is a method of cryptography is used to hide the secret image or information and this process gives the security of information. To hide the data, in steganography cover image is used, in this image the secret information is added.

©IJRASET: All Rights are Reserved

1) It is useful for securely storing delicate information, such as hiding systems password, keys.
2) To transmit secret information, steganography is used as an intelligence

B. A new non Linear Chaotic Algorithm (NCA)

Encryption image is necessary for secure transmission over the internet. Encrypting the picture is traditional algorithm like DES has the flaw of large size image is less efficiency. The chaos represent another algorithm is encryption suggested for new way to get obdurate problem of fast high level security and secure image encryption. The most popular is logistic map and NCA map. Overcome some limits the authors designed NCA map. Limitation of linear functions the authors used power function $(1-x)^{\beta}$ and tangent function. NCA defined as follows.

$$x_{n+1} = (1-\beta^{-4})\cot(\alpha/1+\beta)(1+1/\beta)^{\beta}\tan(\alpha x_n)(1-x_n)^{\beta},$$

Data encrypts image with different keys for different image. Plain picture can be encrypted, it using XOR operation with integer consecution based on NCA using chaotic sequence. Parameters are alpha beta and initial value X0.

Cryptosystem have more practical application and valuable of the chaotic. The proposed NCA presents, image research of information based on the NCA encryption algorithm determined by chaotic system. In this work, secret image encryption is done by using NCA standard in fast analysis.

II. LITERATURE REVIEW

A. September 2018. Introduction, the cloud storage provides the data storage facilities as well as sharing across multiple users. Day by day it's gaining popularity because of enormous benefits. Emerging data security and privacy issues as become a subject to the users as well as service providers. A new efficient embedded least significant bits, and for integrity checking, they use hashing algorithm. First encrypt the data and then hide it in an image to fulfil our purpose. As blowfish is an existing encryption algorithm which is secure enough, so just checkout the steganography methods security. During the quality measurement, they are getting better PSNR value is better than the previously existing methods.

B. **"**New Chaotic algorithm using image encryption" 16 August 2005. Image Encryption Scheme, built on a Non Linear Chaotic Algorithm NCA Proposed an efficient data security method to control data in the cloud storage system using cryptographic. In our paper presents, a new chaotic algorithm (NCA) which uses power function and tangent function instead of linear function. Its structural parameters are alpha beta and initial value x0 obtained by experimental analysis. The experimental analysis demonstrates that the image encryption and decryption algorithm based on NCA.

C. **"**DES image encryption algorithm with LSB encoding technique" 2017. Data by Des encryption algorithm LSB method is not secure enough. They can say that this system doesn't offer better security. An advanced technique to share and protect cloud data using multilayer steganography and cryptography is used. Data is encrypted by AES algorithm. They use only LSB method, in our esteems using E-SLB technique the purpose of secured data.

D. 2005 where for embedding authors used modified LSB together with the raster scan technique. Data security in cloud storage can be increased through cryptography. Data is encrypted by applying any encryption algorithm then store in the cloud server. It is secure but for more sensitive data it is not perfect. Measuring the image quality to get better PSNR values

III. PROPOSED SYSTEM ARCHITECTURE

Architecture setup as shown in the figure which includes the sender and receiver are connected to the respective cloud. Sender reads input file and inserted into cover picture is encrypt and embedded text, original image is encrypted after watermarking image is stored in the cloud. Encrypting data received by the receiver while generating the hash code.

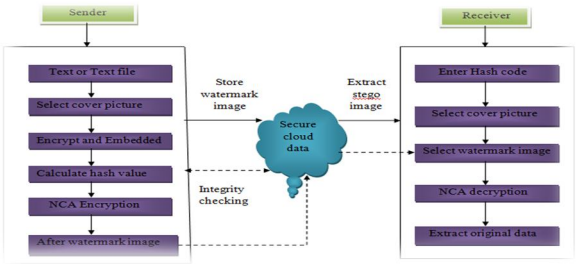


Figure: Designing architecture of the proposed system

©IJRASET: All Rights are Reserved

Sender side select text or text file is converted into characters are converted to ASCII values for example, A is 065. Input text converted into binary numbers 0 and 1 then hiding text to inserted cover picture is encrypt and embedding after generating hash code. Encrypting the data is extracted by the receiver without knowing hash code, using same hash code in the receiver side then it will decrypt and extract the original picture information.

1) *Encryption:* Text or message will be encoded utilizing the NCA encryption calculation.
2) *Implanting:* In this progression we will shroud the scrambled information. Image spread utilizing E-LSB inserting calculation which would make a stego image as a yield.
3) *Hashing:* Here the hash Creation stego picture will be determined utilizing the SHA-256 hashing calculation for checking information respectability in the distributed storage later.
4) *Recovering:* To separate the information from stego image to apply the recovering calculation.
5) *Decoding:* For getting the mystery message the separated information will be unscrambled by NCA decoding calculation.

In the proposed scheme there are basically three options and those are described in below

a) Secure Information Stockpiling In The Cloud: This includes two sections

i) Information Putting Away: For secure information putting away utilize the encryption and the installing calculation.

ii) Information Extraction: For secure information extractions apply to the recovering and the decoding calculation.

b) Information Respectability Check: For checking the trustworthiness data and hash generating stego picture should be determined.

c) Secure Information Partaking In The Cloud: For sharing the information safely it gives sufficient data to the beneficiary so that by utilizing the recovering and the unscrambling calculation the collector can extricate the information from the distributed storage.

IV. E-LSB WITH STEGANOGRAPHY TECHNIQUE

In Embedded least significant bits process all the pixels 8bits of Red Green and Blue plane separately. This procedure is applied we initially scramble the message utilizing NCA encryption strategy. At that point the least noteworthy 3 & 2 bits RGB outline individually. Pixel of the picture will get implanted with the encoded information. We take a character of the encoded information and convert it into 8-bits paired information ASCII esteem at that point conceal 3 least note worthy double information in the R plane next 3 critical bits in the G plane and 2 most huge bits in the B plane individually.

In case we can hide the encrypted message “10101101” RGB plane values of pixel “01101010”, “11101011” and “10001001”. P of 3rd bit consider as left to right for each pixel plane for embedding. This process has shown in Table 1 and Table 2.

Table 1: 8 bits binary frame pixel of the cover image before embedding

01101010	11101011	10001001

The message bits are encrypted: 10101101

01101010	11101010	10001010

Table 2: 8 bits binary frame pixel of the stego image after embedding

In the existing method such as LSB, H-LSB, Modified LSB, anyone can easily extract the hiding data. But in E-LSB that’s why provide the better security than the existing method. The extraction process, we need stego picture only.

V. E-LSB ENCODING WITH NCA ENCRYPTION

Another nonlinear turbulent calculation NCA uses power digression and capacity work rather than direct capacity. Basic parameters are test investigation. Furthermore, a picture encryption calculation in onetime one secret key framework is planned. The exploratory outcomes exhibit that the picture encryption calculation dependent on NCA shows points of interest of huge key space abnormal state security while keeping up worthy productivity. Contrasted and some broad encryption calculations, for example, DES the encryption calculation is increasingly secure.

©IJRASET: All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VIII, Aug 2019- Available at www.ijraset.com

VI. A NEW NONLINEAR CHAOTIC ALGORITHM (NCA)

A. *NCA Map Design*

To conquer those constraints means to plan another nonlinear disorderly calculation NCA. The creators show that turbulent encryption frameworks can be effectively assaulted and security. Reception of nonlinear capacities restricted reality to change the key ceaselessly.NCA use of power $(1 - x_n)^{\beta}$ formula defined as the NCA map

$$x_{n+1} = \lambda.\mathrm{tg}(\alpha x_n).(1 - x_n)^{\beta}, \quad (1)$$

Parameters are λ α and β will be discussed as follows. Slope of the curve at fixed point should not be less than1 and $x_{n+1} > x_n$ when $x_n = (1 + 1/\beta)^{\beta}$ therefore λ defined may be

$$\lambda = \mu.\mathrm{ctg}(\alpha/1 + \beta)\,(1 + 1/\beta)^{\beta}, \mu > 0 \quad (2)$$

Finally, μ is obtained by experimental analysis as a result, $\mu = 1 - \beta^{-4}$. So the NCA map is defined

$$x_{n+1} = (1 - \beta^{-4})\,\mathrm{cot}(\alpha/1 + \beta)\,(1 + 1/\beta)^{\beta}\tan(\alpha x_n)(1 - x_n)^{\beta}, \quad (3)$$

B. *Encryption Algorithm Based on NCA*

1) *Stage 1:* Plain picture sets for the encryption key, with including values of α β and introductory worth X0.
2) *Stage 2:* Do multiple times of tumultuous emphasis as recipe 3 and acquire the decimal portion x100.
3) *Stage 3:* If the encryption work is done, at that point go to stage 6 generally complete multiple times of riotous emphasis and therefore a decimal division, fraction of decimal value is x103 will be created, when its double value we choose only for its first 15 significant digits.
4) *Stage 4:* 15 digits are divided into 5 numbers comprising 3 digits, for every all numbers executes mod 256 activity and another five byte of data will be generated.

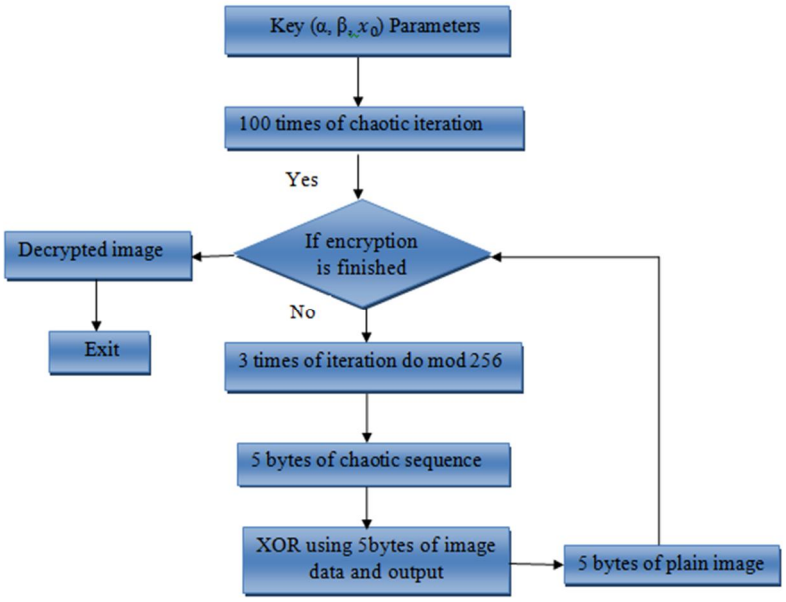


Figure: Flow chart for chaotic encryption algorithm process

5) *Stage 5:* using XOR operation, the five bytes of information with 5 bytes of image information dim worth or shading RGB esteem. Yield the computation result to the article picture and go to stage 3.
6) *Stage 6:* Pass the encoding picture through open correspondence channel.
7) *Stage 7:* encryption key is passed for secure communication channel.
8) *Stage 8:* End.

Calculation of decoding is like encryption calculation however accepting encryption key and working with the encoded picture

©IJRASET: All Rights are Reserved

C. Decryption Algorithm Based on NCA

1) Stage 1: Plain pictures set for the decryption key with the values of α β and introductory worthx_0.

2) Stage 2: Do multiple times of tumultuous emphasis as recipe and acquire the decimal portionx_{100}.

Remaining steps are same as encryption in reverse order like decryption stage 3stage 4 and stage 5

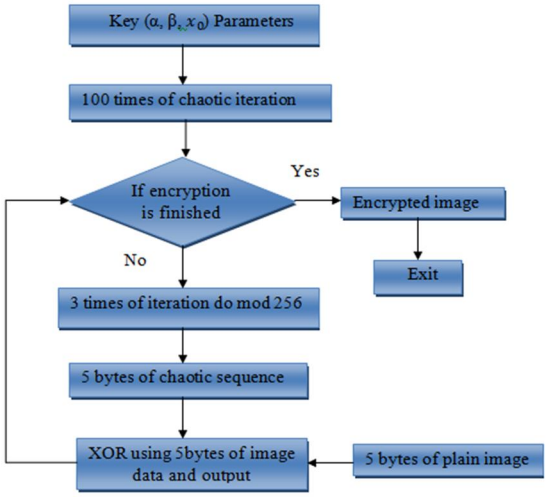


Figure: Flow chart for chaotic decryption algorithm process

3) Stage 6: Pass the decoded picture through open correspondence channel.

4) Stage 7: Decryption key is passed through secure correspondence channel.

5) Stage 8: End.

VII. EXPERIMENTAL ANALYSIS

Encrypted image with the encryption key k=(x_0, α, β) = (0.987654321012345, 1.1, 5) as we can see the encrypted image is rough tumble and unknowable. Figure12 is the decrypted image by the use of decryption algorithm with the same key. It can be clear and correct without any distortion. But if we use wrong key we will not get the image.

Figure 11: Encrypted Cover picture Figure 12: Decrypted watermark picture as stego picture

As expressed before that we are utilizing steganography with encryption for giving cloud data security and protection. For assessing a framework, Peak Signal to Noise Ratio PSNR worth is considered as a parameter. Mean Square Error MSE esteem for figuring PSNR esteem. Condition 3 and condition 4 are utilized to figure esteem separately.

$$MSE = 1/L * H\Sigma_{L,H}[0(L, H) - R(L, H)]^2 \quad (3)$$

Here O (L H) represents cover image, R (L H) represents stego image and L*H denotes the size of the cover image.

$$PSNR=10.\log_{10}(\frac{255*255}{MSE}) \quad (4)$$

For assessing the exhibition of the created framework, we have utilized a few 8-bits RGB pictures as spread pictures and shroud 1KB message in spread pictures. The reenactment has been finished utilizing condition 3 and condition 4. The consequence of the investigation is appeared Table for six example spread pictures with their separate values. A near investigation of various cryptographic calculations for data security in distributed computing is done in. Correlation of the proposed strategy with the two existing strategies based on values for the six example spread pictures is appeared discovered.

©IJRASET: All Rights are Reserved

Scrambled information "11010010" in picture pixel where R="11011110", G= "00110101", and B= "10001001" and we select second piece for installing. Better outcome for our framework.

Example: 256*256 pixels in the spread picture

It very well may be 256*256=65536 Bytes usable bits are implanted

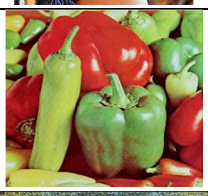
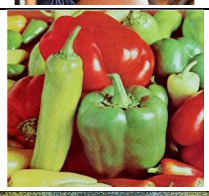
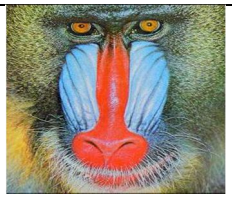
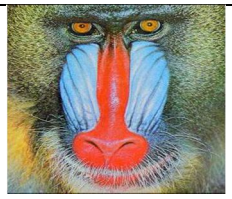
65536*3=196608 Byte can be installed

=24576

=24KB of Data On the off chance that 128*128=16384 it will end up 6KB we can installed.

Subsequent to implanting the information the estimation of that RGB pixel will be R= "1101101" G= "00110101" and B= "10001000". Presently the assailant will get the information "10110100" yet the genuine installed information is "11010010". Think about this framework as a protected framework. So such sort of inadvertent assaults is conceivable.

Table 3: Proposed system

Image Details(256x256)	Cover Image	Stego image	MSE	PSNR (dB)
Airplane .bmp			5.0400e-08	121.1020
Lena .bmp			6.1200e-08	120.2600
Pepper .bmp			5.6800e-08	120.5883
Baboon .ping			5.0900e-08	121.0618
Fruits .ping			505800e-08	120.6606
Cat .ping			7.3400e-08	119.4710

©IJRASET: All Rights are Reserved

VIII. RESULT AND PERFORMANCE ANALYSIS

A. Sender Side

Message
Hema #
Select cover image

Calculating NCA
Text== 13486284145031874
Significant digits after 100 iterations = 134862841450318
Text== 458265429880713
10100010
01101100
11000000
00010001
11101010
Hash Key 1566

B. Receiver Side

P-position = 1566
Extracted text from stego Image

E message = 162 108 192 17 234
Calculating NCA
Text== 13486284145031874
Significant digits after 100 iterations = 134862841450318

IX. CONCLUSION

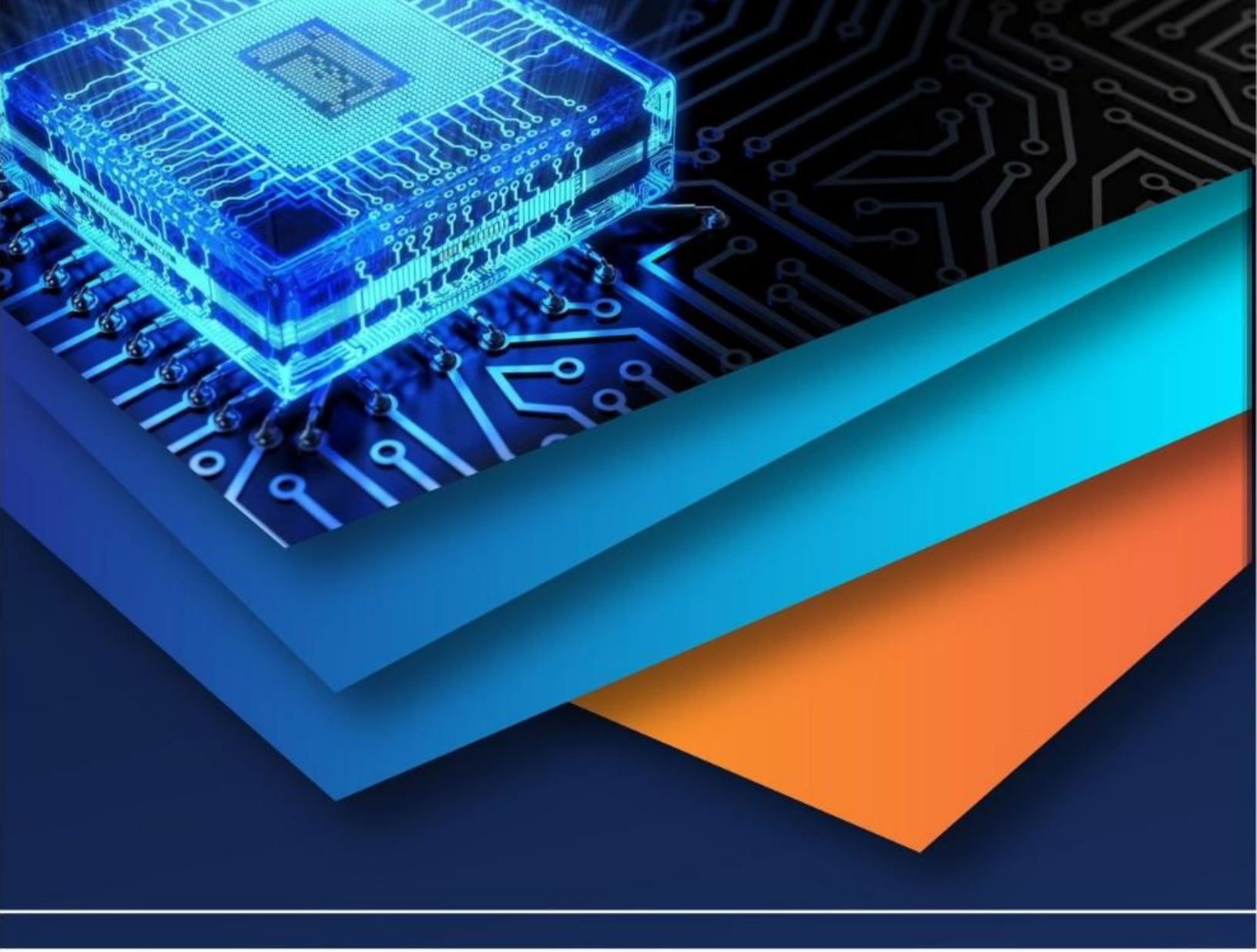
The proposed strategy utilizes the mix of cryptography and picture steganography. For the encoding text, NCA encryption and decryption calculation with E-LSB based steganography is utilized. In the proposed strategy we showed signs of improvement PSNR values in the examination with other existing techniques, which mean our framework, give better regarding security. The developed method can hide and it takes 16KB of data such as message in a cover picture size is 256*256 pixels. The secret picture can be completely covered up in a cover picture by using E-LSB and another secret picture is separated it is difficult to unscramble secret picture. Here likewise utilized the hashing calculation which ascertains stego picture by which can check the respectability data when it is put away in the distributed environment.

©IJRASET: All Rights are Reserved

REFERENCES

[1] S. Nawaz, M. Adib, M. Nawaz, and R. Kamran, "Identifying and analyzing security threats to virtualized cloud computing infrastructures", Proc. of IEEE International Conference on Cloud Computing Technologies, Applications and Managements, pp.151-155, 2012.
[2] B. Karthikeyan, A. Deepak, K. S. Subalakshmi, A. Raj, and V. Vaithiyanathan, "A combined approach of steganography with LSB encoding technique and DES algorithm", Proc. of 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and BioInformatics, 2017.
[3] A. Ranjan, and M. Bhonsle, "Advanced technics to shared & protect cloud data using multilayer steganography and cryptography", Proc. of IEEE International Conference on Automatic Control and Dynamic Optimization Techniques, 2016.
[4] A. Singh, and H. Singh, "An improved LSB based image steganography technique for RGB colour images", Proc. of IEEE International Conference on Electrical, Computer and Communication Technologies, pp.1-4, 2015.
[5] Y. Zhang, C. Xu, X. Liang, and H. Li, "Cryptographic public verification of data integrity for cloud storage system", IEEE Cloud Computing, vol.3, no.5, pp.44-52, 2016.
[6] G. L. Prakash, M. Prateak, and I. Singh, "Efficient data security method to control data in cloud storage system using cryptographic techniques", Proc. of IEEE International Conference on Recent Advances and Innovations in Engineering, pp.1-6, 2014.
[7] Ahmad, J., Hwang, S.O., Ali, A. (2015). An experimental comparison of chaotic and non-chaotic image encryption schemes. Wireless Personal Communications, 84(2), 901–918.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)