An Efficient RC6 based Image Cryptography to Enhance Correlation and Entropy

Apoorva Shrivastava
M.Tech Student
Computer Science, T.I.T, Bhopal

Lokesh Singh
Assistant Professor
Computer Science, T.I.T, Bhopal

ABSTRACT

Security in data communication is a very important concern today. It is used in almost every region like e-commerce, education, and industry and data warehouse. Securely sending and receiving data in the above area is an important as the data is crucial. Image security plays an important role in this age. As the demand of image based message sending is improving day by day. In this paper, we have proposed an efficient image cryptography system based on RC6. The key size and number of variable rounds makes RC6 more secure. The key size is variable up to 2040 bits. The results are achieved in terms of entropy and correlation coefficients. The less variation in entropy is achieved from our approach.

Keywords

Encryption, Chaos, Steganography, Security Measures.

1. INTRODUCTION

With the fast improvements and the data interchanges, a lot of concerns have been brought up in the security of information transmitted or put away over open channels. Particularly at the level of text and picture information. As indicated by [1] there are three fundamental routines for secured correspondence accessible, in particular, cryptography, steganography and watermarking. Among these three, the first one, cryptography [2]-[4], manages the improvement of procedures for changing over data in the middle of understandable and incomprehensible structures amid data trade. Steganography [5]-[6], then again, is a procedure for concealing and separating data to be passed on utilizing a transporter signal [1]. The third one, watermarking [7]-[8], is a method for creating legitimate strategies for concealing restrictive data in the perceptual information.

In [9] authors have recommended that the vast majority of the common pictures, the neighboring's estimations pixels are unequivocally associated (i.e. the estimation of any given pixel can be sensibly anticipated from the estimations of its neighbors [10]-[12]. So keeping in mind the end goal to accomplish the higher relationship entropy among pixels and expanding the entropy quality is a developing examination range. In case of text the data should be hiding with images so that more security will impose with RGB combinations and variations.

In [13] the most critical issues, which influence the mainstream data of advanced media, are the way to secure theft and possession. The watermarking of the prevalent methodologies considers ding as a new database for giving the copyright insurance, is a procedure in view of implanting a particular imprint or mark into the computerized items. While a few watermarking calculations have been proposed [14] in this heading.

So in the ensuing segment we talk about data encryption method for picture encryption. We additionally talk about the pivotal angles which are utilized as a part of picture encryption with their points of interest and drawbacks. At long last taking into account the discourses we additionally recommend some future comment which may be productive in this bearing.

There are niacumerous essential techniques which are second-hand pervasive cryptography, for example, private or mystery key cryptography, open fundamental or kilter, computerized mark, and hash capacities [15]. In private key cryptography, a solitary key is leftover for both encryption and decoding. This obliges meander if all else fails part convey offering an impersonation of the key and the key be struck by be passed swear off a safe channel to the next individual [13-22]. Private-key calculations are level indestructible and effectively actualized in equipment. Along these lines they are over and again second-hand for mass measurements encryption. The vast please of the all-around adjusted encryption rely on upon plaintext, encryption calculation, key and unscrambling calculation. The plaintext is the size ahead requiring the encryption calculation. It is joining of the inputs to the encryption calculation. The encryption calculation is the calculation used to continue on b deal with the information stranger plaintext to figure relieve. The mystery key is a comparable to repel of the encryption calculation and of the plaintext and it is associate of the encryption's inputs calculation [23][24]. The figure content is the defiant content discover as yield [14][15]. The steganography technique with cryptography will enhance the security as the cryptic content and the randomization quality can be improved.

2. LITERATURE SURVEY

In 2005,Zhi-Hong Guan et al. [25] have introduced another picture encryption plan, in which rearranging the positions and changing the dark estimations of picture pixels are joined to confound the relationship between the figure picture and the plain picture. In 2013, Praloy Shankar De et al. [26] endeavor has been made to concentrate on a calculation of cryptography that was made by utilizing old philosophies. DEDD Symmetric-key cryptosystem is the new way to deal with symmetric key calculation. By this technique they can doubly scramble and doubly decode the message. It implies the sender will produce the figure content from the plain content twice. The beneficiary will likewise need to decode the figures for two times and afterward the correspondence between them will be finished. For creating the key, they will take the message length in first encryption and in second encryption they will apply moving system. In 2013, Seetaiah Kilaru et al. [27] propose that security is the principle worry in any field. With the successive assaults, it is a major test for the clients to secure the advanced pictures which are transmitting over web. Solitary Value Decomposition (SVD) gives an answer up to a more prominent degree. Creator proposes that by utilizing the Wavelets, undetectable watermark insert into the first watermark. The fundamental center focused on the remote interchanges; subsequently it is vital to think of some as components into thought, they are size of a picture and prerequisites of data transfer capacity. Keeping in perspective of every one of these parameters, pressure and transmission ought to be finished. In 2012, Long Baoa et al. [28] proposed disordered framework indicates fantastic turbulent practices. To exhibit its application in picture preparing, another picture encryption plan utilizing the proposed disordered framework is likewise presented. PC reproduction and security investigation exhibit that the proposed picture encryption plan indicates phenomenal encryption execution, high affectability to the security keys, and an adequately huge key space to oppose the savage assault. In any case, in this paper irregular like nature of disarray is not considered. In 2012, Abusukhon et al. [29] proposed a novel method for data encryption which is able to transformation file into an image file on both sides of system that is client and server. They have analyzed their algorithm by exploring the number of all possible key permutations. In 2014, Mostaghim et al. [30] suggest making the visual cryptography more robust which can able to share sent and the received data with the generated message and will combine to the received share to reveal the hidden message. Their proposed scheme is evaluated in terms of Histogram, correlation coefficient, key sensitivity and key space. Their results are found to be improved in comparison to the traditional technique. In 2015, Hassan et al. [31] proposed a secure communication scheme. It is a hyperchaotic system used as a carrier for the encoded data to be transmitted. At the transmitter end, two diverse disorganized frameworks are coupled and used to build another hyperchaotie framework. One of the yields of the hyperehaotie framework is utilized as a bearer for the scrambled information. At the less than desirable end, the discrete-time Regularized Least Square (RLS) estimator is utilized to remake the disorderly flag and consequently recover the encoded information. Their reproduction results are representing the viability of the proposed methodology. In 2015, Li et al. [32] integrated the concept of session key establishment and extended chaotic maps for the fulfillment to allow data senders and data receivers to establish a secure common session key through a trusted server over an insecure channel. They proposed a secure three-party authenticated key exchange protocol (3PAKE) which is based on extended chaotic maps in storage service without using smart card and timestamp. It requires neither long-term secret keys nor symmetric cryptosystems. It fulfills the protection requirement against various attacks. Their proposed protocol is more secure and practical for real environments. Security in different aspects is also suggested in [33]. In 2015, Haroun et al. [34] presented a key generation method which is based on the wireless fading channels. It is employed based on the broadband chaotic signal for data transmission so that it is frequency selective. Their proposed calculation misuses this property to produce an one of a kind shared key between two gatherings. The no periodicity of the turbulent sign gives an extraordinary sign to key era, which can be utilized even with static blurring channels. Their proposed methodology is powerful to timing contrasts between the gatherings in light of the fact that the recurrence range of the signs is utilized. The key's irregularity is affirmed, and the impacts of added substance white Gaussian clamor and timing contrasts on the calculation's execution are inspected. In [35] authors has suggested single sign-on (SSO) concept for authorization and login and it proves to be good to any enterprise solution.

3. PROPOSED WORK

In this paper we have proposed an efficient image cryptography method by using RC6 algorithm. Our work is categorized by the following five steps. It can also be better understood from the figure 1.

Design

Our framework is consisting of java pages which are mainly used for designing the framework of image cryptography, histogram calculation, and entropy measurement and correlation analysis. This framework is created in Netbeans7.2 environment.

Data Preprocessing

We have considered Leena and other images from the database. This data is the plaintext for the next processing.

Data Encryption

Image data is first converted in the 2D array. Then RC6 algorithm is applied for data encryption process. This process is applied according to the algorithm 1.

First a key of length k bytes and the 128-piece plaintext square is stacked into words A; B ; C; and D beginning with the low-arrange byte of A. These four w-bit words contain the yield figure content toward the end. Here we portray encryption and unscrambling. RC6 works with four w-bit enlists A; B ; C; D which contain the beginning info plaintext and in addition the yield figure content toward the end of encryption. The main byte of plaintext or figure content is put at all critical byte of A; the last byte of plaintext or figure content is set into the hugest byte of D. We utilize (A; B ; C; D)=(B; C; D; A) to mean the parallel task of qualities on the privilege to enrolls on the left.

Image XOR

Five different key images are used randomly for the XOR operation. XOR is a binary operation, it remains for "select or", that is to say the subsequent piece assesses to one if just precisely one of the bits is set. This operation is performed between each two relating bits of a number for data shuffling.

Histogram

Black and white histogram with RGB histogram is computed for observing the changes in the RGB combination. It provides bin comparison point by point.

Data Decryption

The reversible process is applied for retrieving the data after encryption for decoding component with the different keys for a single file in many trials. The RC 6 key is applied for data decryption. It is secured by the encryption secret key.

Entropy

The entropy is the measurement of information loss in the process of encryption and decryption. The probability of symbol is 1. The value of entropy is calculated by the below formula.

$\sum_{i=1}^{n} 1 - p(s_i)\log_2 p(s_i)$ Entropy (H) is:

Correlation coefficient analysis

The correlation coefficient is a numerical approach to evaluate the relationship between two variables. Let P and Q and it is signified by the image R. The correlation coefficient is dependably between -1 and 1, thus -1 < R < 1. If the correlation coefficient, R, is positive, then an expansion in P would result in an increase in Q, however if R was negative, an expansion in P would result in a decrease in Y. Bigger connection coefficients, for example, 0.8 would recommend a more grounded relationship between the variables, whilst figures like 0.3 would propose weaker ones.

However, the correlation coefficient does not infer causality that is it might demonstrate that two variables are firmly corresponded; anyway it doesn't imply that they are responsible for one another. Points of interest of the relationship coefficient are that it is anything but difficult to work out and it's simple to translate.

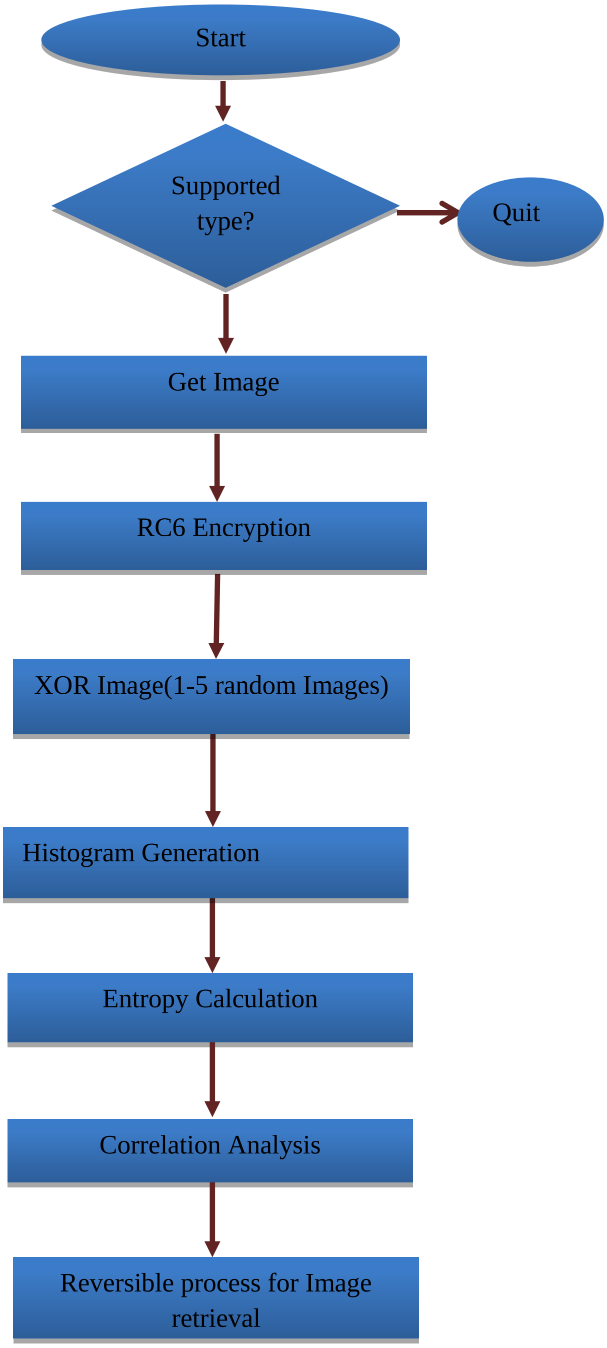

Figure 1: Flowchart

Algorithm 1[65]:

```
Step 1: Image is converted into 2D array.
Step 2: It is stored in the array.
Step 3: Number r of rounds [all the initialization is random]
x = First initialization
y = Second initialization
Yield:
Step 4: w-bit round keys S[0,… , 2r + 3]
Strategy:
S[0] = x
Step 5: for i = 1 to (2r + 3) do
        S[i] = S[i - 1] + y
Step 6: Each block key is generated until reached to the end of file vector.
Step 7: Shifting process
A = S[i] = (S[i] + A + B) <<< 3
Step 8: Then again shifting is performed with the 3 bit java shifting to make the substitution matrix.
Step 9: The whole process is applied to the whole block division achieved.
Step 10: The final key is generated according to the r rounds.
Step 7: End;
```

Algorithm 2: Correlation Analysis

Abbreviations:
LC=Linear Correlation
VC=Vertical Correlation
HC=Horizontal Correlation
Corr= Correlation

```
Step 1: if type == LC
for (i=0; i<nrows; i++)
for (j=0; j<ncols; j++)
corr += arr1[i][j] * arr2[i][j];
corr /= size;
   }
else if type == VC
for (i=0; i<nrows; i++)
for (j=0; j<ncols; j++)
mag1 += arr1[i][j] * arr1[i][j];
mag2 += arr2[i][j] * arr2[i][j];
corr += arr1[i][j] * arr2[i][j];
corr /= Math.sqrt(mag1*mag2);
else
for i=0; i<nrows; i++
for (j=0; j<ncols; j++)
mean1 += arr1[i][j];
mean2 += arr2[i][j];
mean1 /= size;
mean2 /= size;
Step 2:for i=0; i<nrows; i++
for j=0; j<ncols; j++
arr1[i][j] -= mean1;
arr2[i][j] -= mean2;
mag1 += arr1[i][j] * arr1[i][j];
mag2 += arr2[i][j] * arr2[i][j];
corr += arr1[i][j] * arr2[i][j];
corr /= Math.sqrt(mag1*mag2);
```

4. RESULT ANALYSIS

In the result section we have discussed the results obtained from different prospective to validate the outcomes. For the experimentation we have considered the leena image. First we have applied RC 6 encryption on the said image. Then XOR is performed according to the 5 random images available in our database. The results based on the above phenomena are shown in figure 2. The RGB color combination obtained from the original picture, encrypted image and XOR image is shown in figure 3, 4 and 5 respectively. The correlation coefficient is then calculated for the original, encrypted and XOR image. It is between -1 and 1. The less difference in correlation suggest better connection coefficient. In case of our approach as shown in table 1, figure 6 and 7 it is higher with less difference in comparison to the previous approach. We have also calculated the information entropy to check the loss in information when cryptography is performed. The results in table 2 shows very less difference which shows less information loss by our approach.

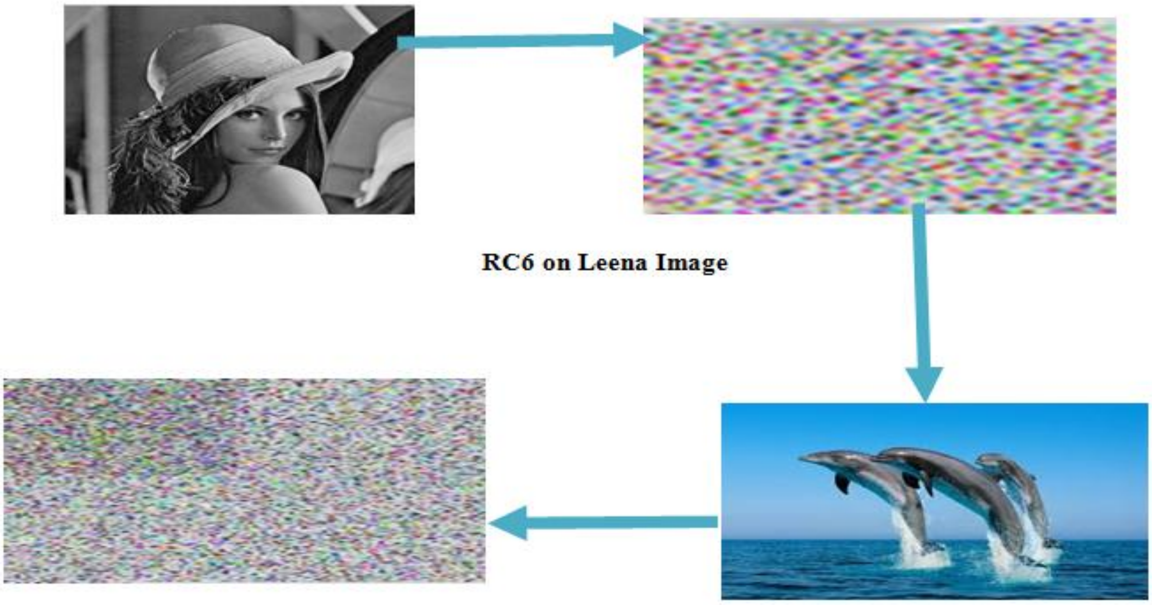

Figure 2: RC6 + XOR on Leena Image

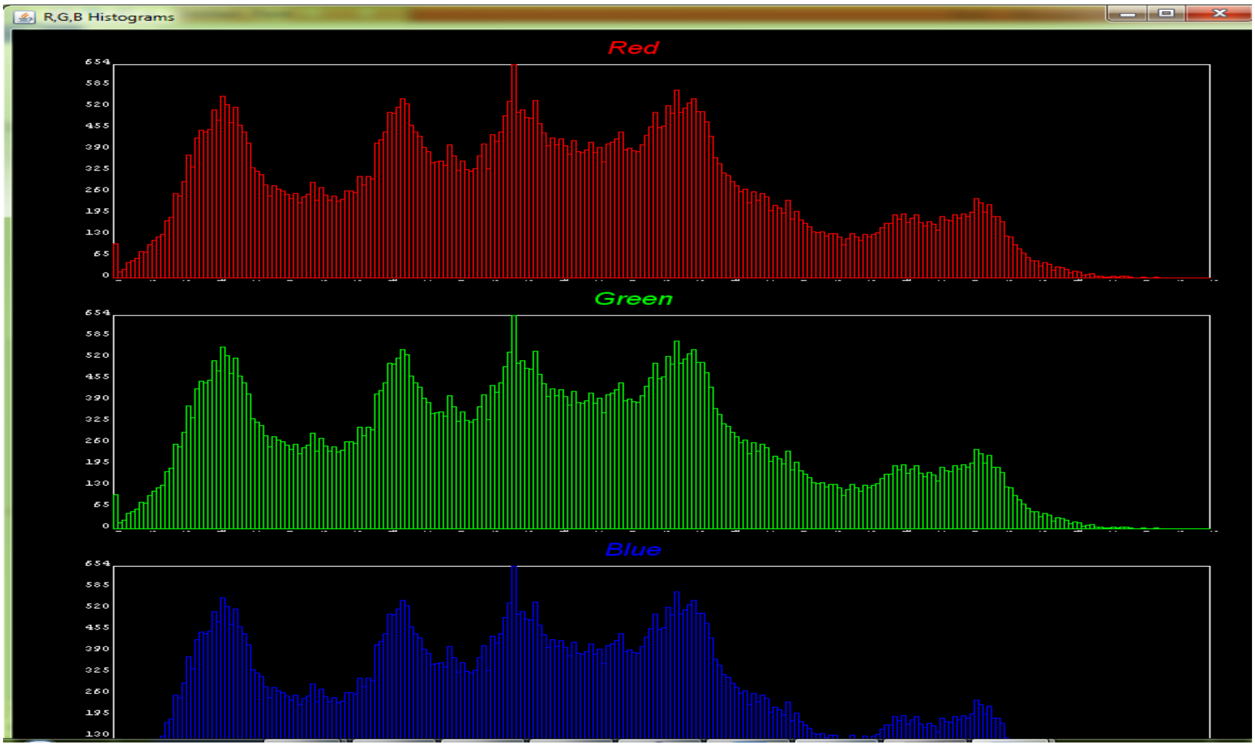

Figure 3: RGB combination of Leena Original Image

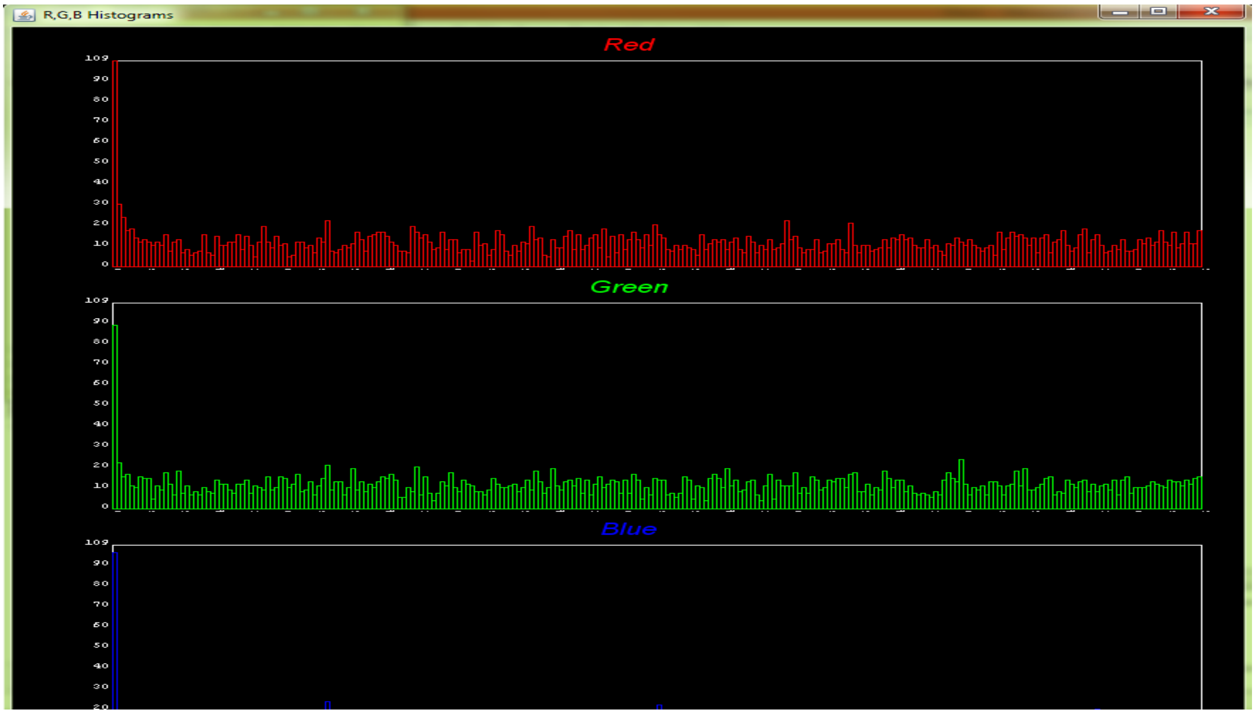

Figure 4: RGB combination of Leena Encrypted Image

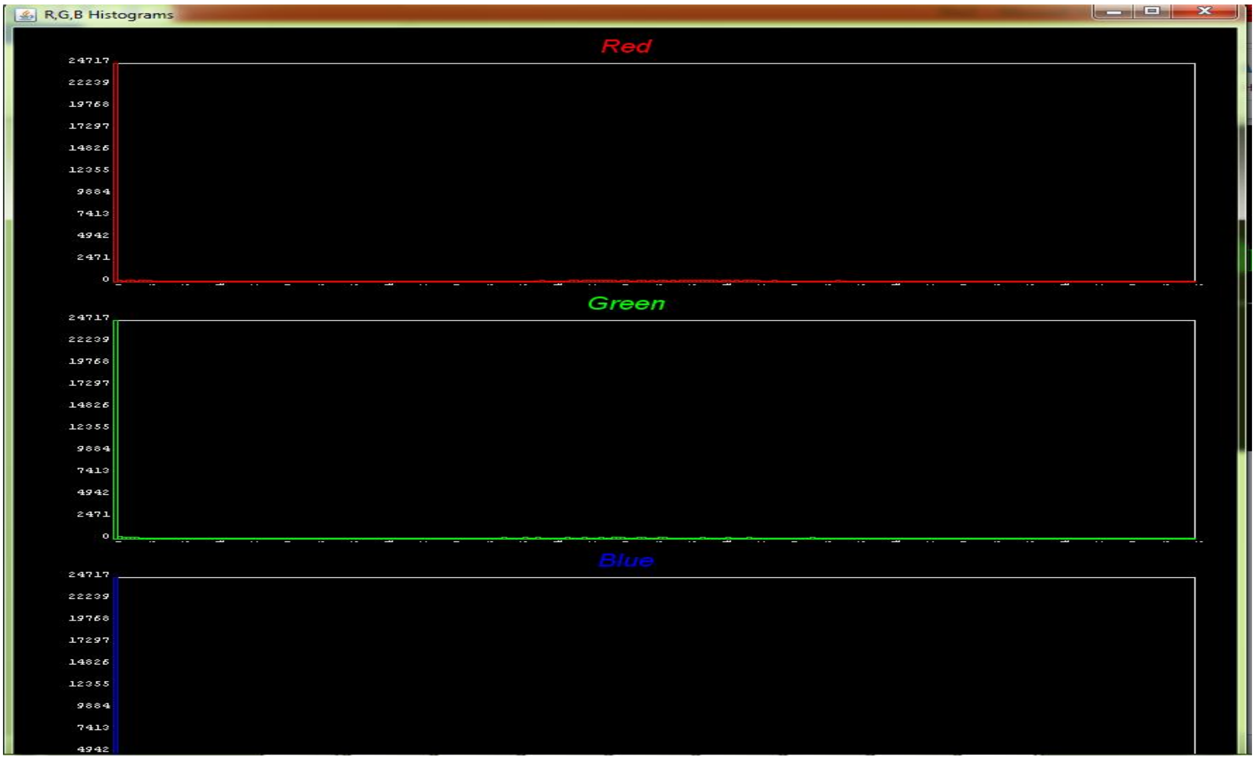

Figure 5: RGB combination of Leena XOR Image

Table 1: Correlation Analyscis(proposed work)

Methods	Leena Image	Chaotic Share	Secret Image(XOR)
Vertical Correlation(VC)	1	0.98	0.96
Horizontal Correlation(HC)	1	0.69	0.57
Normal Correlation	56531.76	55478.02	52771.47

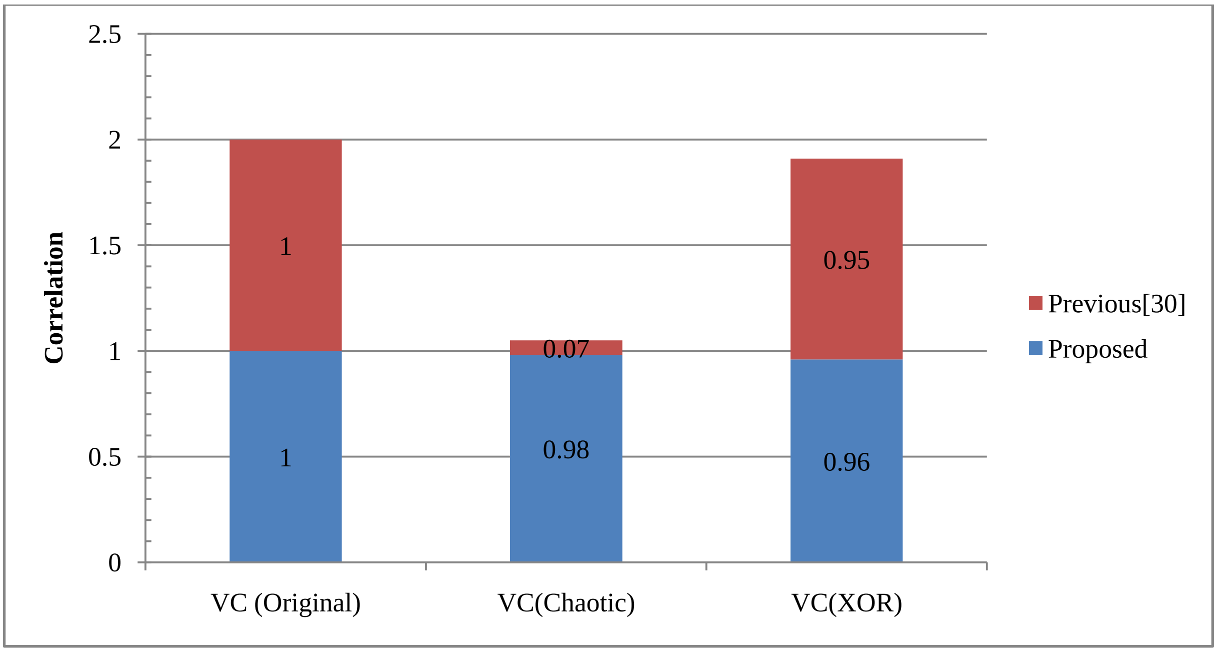

Figure 6: Comparison of proposed work (Vertical Correlation) with [30]

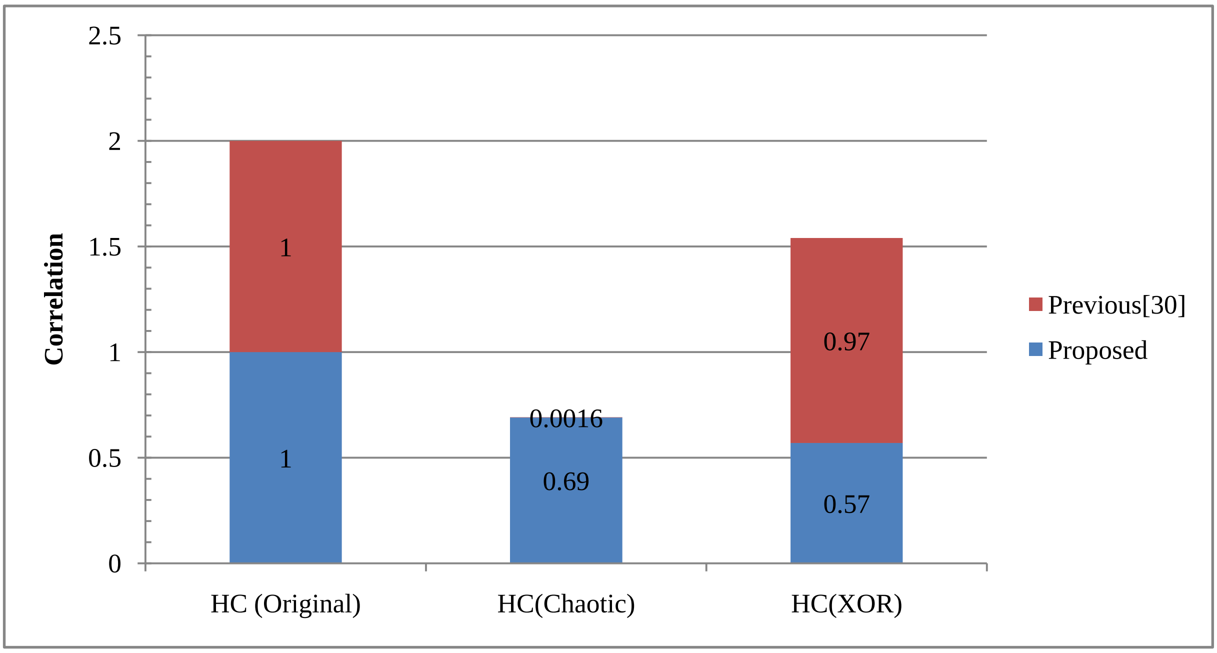

Figure 7: Comparison of proposed work(Horizontal correltion) with [30]

Table 2: Information Entropy

Image Name	Entropy for Original Image	Entropy for Encrypted Image
Leena Image	7.93	7.98
Cameraman Image	7.95	7.98
Barbara Image	7.95	7.99
African Man	7.96	7.99
Mountain	7.97	7.98
Elaine	7.92	7.98

5. CONCLUSION

This paper provides a security framework for image database. Based on the analysis and observations we have used encryption technique RC6. RC6 is used as its provides key size variability so the security is improved. Then we have applied XOR to enhance the image mapping and security so that confusion matrix is not easily detectable. The results are first compared with the RGB combination which shows significant difference in the original, encrypted and XOR image. Then correlation coefficient is compared with the previous result and shows better correlation in terms of previous method. For observing information loss we have calculated entropy, the variation in the entropy is very less which shows that the information loss is negligible.

6. REFERENCES

[1] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol. 1, no. 1, p.127, 2006.

[2] A. J. Elbirt and C. Paar, “An Instruction-Level Distributed Processor for Symmetric-Key Cryptography,” IEEE Trans. Parallel and distributed systems, vol. 16, no. 5, pp. 468-480, May 2005.

[3] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Trans. Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[4] W. Stallings, Cryptography and Network Security. Englewood Cliffs,NJ: Prentice Hall, 2003.

[5] E. Besdok, “Hiding information in multispectral spatial images,” Int. J.Electron. Commun. (AEU) 59, pp. 15-24, 2005.

[6] S. Trivedi and R. Chandramouli, “Secret Key Estimation in Sequential Steganography,” IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 746-757, Feb. 2005.

[7] Y. Wu, “On the Security of an SVD-Based Ownership Watermarking,”IEEE Trans. Multimedia, vol. 7, no. 4, pp. 624-627, Aug. 2005.

[8] Y. T. Wu and F. Y. Shih, “An adjusted-purpose digital watermarking technique,” Pattern Recognition 37, pp. 2349-2359, 2004.

[9] Mohammad Ali Bani Younes and Aman Jantan,” Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.

[10] S. P. Nana'vati., P. K. panigrahi. "Wavelets:applications to image compression- I,". joined of the scientific and engineering computing, vol. 9, no. 3, 2004, pp. 4- 10.

[11] c. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.

[12] AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo,"Video over IP using standard-compatible multiple description coding," Journal of Zhejiang University- Science A, vol. 7, no. 5 ,2006, pp. 668- 676.

[13] Neha Chauhan, Akhilesh A. Waoo, P. S. Patheja,” Attack Detection in Watermarked Images with PSNR and RGB Intensity”, International Journal of Advanced Computer Research (IJACR) Volume-3 Number-1 Issue-9 March-2013.

[14] G. Voyatzis, N. Nikolaidis and I. Pitas, “Digital watermarking: An overview”, EUSIPCO, vol. 1, pp. 9-12, 1998.

[15] Shikha Joshi, Pallavi Jain,” A Secure Data Sharing and Communication with Multiple Cloud Environments with Java API”, International Journal of Advanced Computer Research (IJACR) Volume 2 Number 2 June 2012.

[16] A. Sinha, K. Singh, “A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2003.

[17] Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., Bourbakis Fellow., IEEE. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004.

[18] Satish Bhalshankar and Avinash K. Gulve, " Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes “, International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-20, September-2015, pp.233-248.

[19] Nanda Hanamant Khanapur and Arun Patro, “Design and Implementation of Enhanced version of MRC6 algorithm for data security ", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015, pp.225-232.

[20] Sridevi and Manajaih.D.H, “Modular Arithmetic in RSA Cryptography”, International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-17, December-2014, pp.973-978.

[21] Dubey, Ashutosh Kumar, et al. "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment." Software Engineering (CONSEG), 2012 CSI Sixth International Conference on. IEEE, 2012.

[22] Tavse, Priyanka, and Anil Khandelwal. "A Critical Review on Data Clustering in Wireless Network." International Journal of Advanced Computer Research (IJACR) 4 (2014): 795-798.

[23] Nath, Asoke, et al. "Multi Way Feedback Encryption Standard Ver-2 (MWFES-2)." International Journal of Advanced Computer Research (IJACR) 3.1 (2013).

[24] Namrata Shukla, “Data Mining based Result Analysis of Document Fraud Detection”, International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 ,pp.21-25.

[25] G. Zhi-Hong, H. Fangjun, and G . Wen ie , " Ch aos - based image encryption algorithm,"Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.

[26] Praloy Shankar De, Prasenjit Maiti,” DEDD Symmetric-Key Cryptosystem”, International Journal of Advanced Computer Research (IJACR) ,Volume-3 Number-1 Issue-8 March-2013.

[27] Seetaiah Kilaru, Yojana Kanukuntla, K B S Chary,” An effective algorithm for Image security based on Compression and Decomposition method”, International Journal of Advanced Computer Research (ISSN (IJACR) Volume-3 Number-1 Issue-8 March-2013.

[28] Long Bao, Yicong Zhou,C. L. Philip Chen," A New Chaotic System for Image Encryption", 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China.

[29] Abusukhon, Ahmad, and Mohammad Talib. "A novel network security algorithm based on private key encryption." Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. IEEE, 2012.

[30] Mostaghim, Melika, and Reza Boostani. "CVC: Chaotic visual cryptography to enhance steganography." Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on. IEEE, 2014.

[31] Hassan, Mohamed Fahim. "Synchronization of hyperchaotic systems with application to secure communication." Systems Conference (SysCon), 2015 9th Annual IEEE International. IEEE, 2015.

[32] Li, Chun-Ta, Chin-Wen Lee, and Jau-Ji Shen. "A secure three-party authenticated key exchange protocol based on extended chaotic maps in cloud storage service." Information Networking (ICOIN), 2015 International Conference on. IEEE, 2015.

[33] Dubey, A. K., Dubey, A. K., Agarwal, V., & Khandagre, Y. . Knowledge discovery with a subset-superset approach for Mining Heterogeneous Data with dynamic support. In Software Engineering (CONSEG), 2012 CSI Sixth International Conference on (pp. 1-6). IEEE.

[34] Haroun, M.F.; Gulliver, T.A., "Secret Key Generation Using Chaotic Signals Over Frequency Selective Fading Channels," in Information Forensics and Security, IEEE Transactions on , vol.10, no.8, pp.1764-1775, Aug. 2015.

[35] Hsien-Yu Lee and Nai-Jian Wang, "The implementation and investigation of securing web applications upon multi-platform for a single sign-on functionality", International Journal of Advanced Computer Research (IJACR), Volume-6, Issue-23, March-2016 ,pp.39-46.

[36] Rivest RL, Robshaw MJ, Sidney R, Yin YL. The RC6TM block cipher. InFirst Advanced Encryption Standard (AES) Conference 1998 Aug 20.