

An Enhanced Secure Image Cryptography based on RC6 and RSA to Minimize Entropy and Improve Correlation

Pooja Chaturvedi, Chetan Gupta

Department of CSE

M.Tech (Scholar), SIRTS

poojachaturvedi55@gmail.com

Department of CSE

Asst. Prof. SIRTS

chetangupta.gupta1@gmail.com

Abstract— a secure environment would not be possible without the existence of encryption technology. Image, which covers the large percentage of the multimedia data, its protection is very important in a current scenario. So focusing the security possibility an efficient image cryptography system based on RC6 and RSA have been proposed in this paper. The specialty of this approach is the number of keys. There are four different keys are needed for decryption process along with the extra shifting of pixels by XOR. The key size and number of variable rounds makes this framework 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 which shows the efficiency of our approach.

Keywords– Encryption, RSA, RC6, Entropy, Correlation Coefficient

of embedding a specific engraving or check into the modernized things. While a couple watermarking computations have been proposed [14] in this heading.

1. Introduction

With the quick enhancements and the information exchanges, considerable measures of concerns have been raised in the security of data transmitted or set away over open channels. Especially at the level of content and picture data. As showed by [1] there are three essential schedules for secured correspondence open, specifically, cryptography, steganography and watermarking. Among these three, the first one, cryptography [2]-[4], deals with the change of systems for changing over information amidst reasonable and unlimited structures in the midst of information exchange. Steganography [5]-[6], on the other hand, is a strategy for hiding and isolating information to be gone on using a transporter signal [1]. The third one, watermarking [7]-[8], is a technique for making genuine systems for disguising prohibitive information in the perceptual data.

In [9] creators have prescribed that most by far of the regular pictures, the neighboring's estimations pixels are unequivocally related (i.e. the estimation of any given pixel can be sensibly expected from the estimations of its neighbors [10]-[12]. So remembering the final objective to achieve the higher relationship entropy among pixels and extending the entropy quality is a creating examination range. In the event of content the information ought to be covering up with pictures so that more security will force with RGB mixes and varieties.

In [13] the most basic issues, which impact the standard information of cutting edge media, are the best approach to secure robbery and ownership. The watermarking of the common strategies consider ding as another database for giving the copyright protection, is a technique in perspective

So in the resulting fragment we discuss information Encryption strategy for picture encryption. We also discuss the significant edges which are used as a piece of picture encryption with their purposes of hobby and downsides. Finally considering the talks we also suggest some future remark which might be beneficial in this bearing.

There are various key strategies which are second-hand pervasive cryptography, for instance, private or puzzle key cryptography, open central or kilter, automated check, and hash limits [15]. In private key cryptography, a single key is remaining for both encryption and interpreting. This obliges wind when in doubt part pass on offering a mimic of the key and the key be struck by be passed swear off a sheltered channel to the following individual [13-22]. Private-key algorithms are level indestructible and adequately completed in gear. Thusly they are on and well actually for mass estimations encryption. The limitless please of the inside and out balanced encryption depend on upon plaintext, encryption computation, key and unscrambling count. The plaintext is the size ahead requiring the encryption figuring. It is joining of the inputs to the encryption figuring. The encryption count is the computation used to proceed and manage the data stranger plaintext to figure mitigate. The secret key is a practically identical to repulse of the encryption computation and of the plaintext and it is partner of the encryption's inputs count [23][24]. The figure substance is the rebellious substance find as yield [14][15]. The steganography procedure with cryptography will upgrade the security as the obscure substance and the randomization quality can be progressed.

2. Literature Survey

In 2005, Zhi-Hong Guan et al. [25] have presented another picture encryption arrangement, in which improving the positions and changing the dull estimations of picture pixels are joined to bewilder the relationship between the figure picture and the plain picture.

In 2013, Praloy Shankar De et al. [26] try has been made to focus on a count of cryptography that was made by using old rationalities. DEDD Symmetric-key cryptosystem is the better approach to manage symmetric key estimation. By this strategy they can doubly scramble and doubly translate the message. It infers the sender will create the figure content from the plain substance twice. The recipient will in like manner need to disentangle the figures for two times and a short time later the correspondence between them will be done. For making the key, they will take the message length in first encryption and in second encryption they will apply moving framework.

In 2013, Seetaiah Kilaru et al. [27] suggest that security is the guideline stress in any field. With the Progressive strikes, it is a noteworthy test for the customers to secure the propelled pictures which are transmitting over web. Lone Value Decomposition (SVD) surrenders a response to a more noticeable degree. Maker recommends that by using the Wavelets, imperceptible watermark embed into the principal watermark. The major focus concentrated on the remote trades; in this manner it is imperative to think about some as segments into thought, they are size of a photo and essentials of information exchange limit. Keeping in context of each one of these parameters, weight and transmission should be done.

In 2012, Long Baoa et al. [28] proposed confused structure shows fabulous turbulent practices. To show its application in picture get ready, another picture encryption arrangement using the proposed cluttered system is moreover introduced. PC generation and security examination display that the proposed picture encryption arrangement shows marvelous encryption execution, high affectability to the security keys, and an enough gigantic key space to contradict the savage attack. Regardless, in this paper sporadic like nature of disorder is not considered.

In 2012, Abusukhon et al. [29] proposed a novel strategy for information encryption which can change record into a picture document on both sides of framework that is customer and server. They have broken down their calculation by investigating the quantity of all conceivable key stages.

In 2014, Mostaghim et al. [30] recommend making the visual cryptography more hearty which can ready to impart sent and the got information to the produced message and will consolidate to the got offer to uncover the shrouded message. Their proposed plan is assessed as far as Histogram, connection coefficient, key affectability and key space. Their outcomes are observed to be enhanced in contrast with the customary procedure.

In 2015, Hassan et al. [31] proposed a protected correspondence plan. It is a hyper disordered framework

utilized as a bearer for the encoded information to be transmitted. At the transmitter end, two various disrupted structures are coupled and used to manufacture another hyper tumultuous system. One of the yields of the hyper disordered system is used as a carrier for the mixed data. At the not exactly alluring end, the discrete-time Regularized Least Square (RLS) estimator is used to redo the jumbled banner and thusly recoup the encoded data. Their propagation results are speaking to the suitability of the proposed procedure.

In 2015, Li et al. [32] coordinated the idea of session key foundation and broadened confused maps for the satisfaction to permit information senders and information recipients to build up a protected normal session key through a trusted server over a frail channel. They proposed a protected three-party confirmed key trade convention (3PAKE) which depends on amplified turbulent maps away administration without utilizing savvy card and timestamp. It requires neither long haul mystery keys nor symmetric cryptosystems. It satisfies the assurance necessity against different assaults. Their proposed convention is more secure and commonsense for genuine situations.

In 2015, Haroun et al. [33] introduced a key era technique which depends on the remote blurring channels. It is utilized in view of the broadband turbulent sign for information transmission with the goal that it is recurrence specific. Their proposed estimation abuses this property to create a unique shared key between two social affairs. The no periodicity of the turbulent sign gives a phenomenal sign to key time, which can be used even with static obscuring channels. Their proposed philosophy is intense to timing contrasts between the social affairs in light of the way that the repeat scope of the signs is used. The key's anomaly is certified, and the effects of included substance white Gaussian uproar and timing contrasts on the figuring's execution are investigated. The key based security and analysis is also presented with the problems in [34, 35, 36].

In 2015, Zaher et al. [37] proposed a new technique for secure correspondence that goes for robustifying established Chaotic Shift Keying (CSK) methods. A novel cryptography calculation is utilized to change the transmitter parameters such that they have a fourfold frame; along these lines, breaking into people in general correspondence channel utilizing return map assaults will come up short. At the recipient side, a versatile control strategy is utilized to assess the time-differing transmitter parameters through receiving a complete synchronization approach. Reenactment results illustrate the prevalent execution of the proposed method in both time and recurrence spaces. A Duffing oscillator is utilized to fabricate the proposed framework utilizing just the time arrangement for the yield. Different implementation issues are investigated for various digital multimedia data and an experimental investigation is carried out to verify the effectiveness of the proposed technique.

In 2015, Kharat et al. [38] proposed a three differential mayhem based straightforward encryption and information concealing system in which first time confusion is utilized for position stage and esteem change. With the assistance of this calculation they can accomplish high security reason. Intricacy of calculation is lessened by disposing of any progression from calculation for low medium. In any case, with the assistance of result they have demonstrated that this calculation is best for any attack.

3. Proposed Work

In this paper we have proposed an efficient image cryptography method by using RSA and RC6 algorithm. It can also be better understood from the figure 1. 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. We have considered different images and other images from the database. This data is the plaintext for the next processing. We also consider the database of James Z. Wang which is the collection of 1000 Databases. There are 10 categories in the database including African men, seas, Buildings, Buses, dinosaur, elephant, roses, horses, mountains and food. In this paper the above mentioned images are use and want to show information loss comparison between the traditional chaos's based system and our proposed system.

Algorithm for Java based Permutation

Step 1: Take a String Variable;
 Step 2: Consider the object image and convert it into string variable;
 Step 3: Create a double dimension integer array;
 int arr[][];
 Step 4: Make an object for Image to 2D Conversion;
 Step 5: Pass it in terms of object to get the conversion;
 Step 6: Loop is considered in row and column
 for i=0 to array.length;
 for j=0 to array.length;
 append string values in terms of numeric content.
 Step 7: Finally the data will be appended.
 Step 8: append text area.

RSA Algorithm:

The encryption key (e,n), is calculated in the following way:
 Step 1: The public/private key pair is generated by the following steps:
 Choose two large primes at random – a,b
 Step 2: Caculate system modulus $N=a.b$
 $\phi(N)=(a-1)(b-1)$
 Step 3: Encryption key e is now choosen in this manner that the e lies in $1 < e < \phi(N)$, $\gcd(e, \phi(N))=1$
 Step 4: Decryption key d is calculated then $e.d=1 \pmod{\phi(N)}$ and $0 \leq d \leq N$
 Step 5: public encryption key: $KU=\{e,N\}$
 Step 6: private decryption key: $KR=\{d,a,b\}$
 Step 7: For encrypting the message M first receive the public key of the receiver: $KU=\{e,N\}$

$C=Me \pmod N$, where $0 \leq M < N$

Step 8: For decrypting it use the private key $KR=\{d,a,b\}$
 $M=Cd \pmod N$

Algorithm RC6

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 $S[0, \dots, 2r + 3]$
 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
 $A = S[i] = (S[i] + A + B) \lll 3$
 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;

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.

Then we apply java based XOR operation so that the image will be more distorted and pixel will be shuffle.

Java based XOR:

Step 1: Consider random images in a string array;
 Step 2: Random images are selected for XOR operation;
 r.nextInt(5);
 Step 3: Consider the substring value with the same pixel form staring to the final length;
 Step 4: Make an object for the above substring;
 Step 5: Pass it in terms of object;
 Step 6: Loop is considered in row and column
 for j=0 to length-1;
 Find the substring
 The above procedure will be parsing up to the final length;
 Step 7: Finally Image will be appended based on height width specified.
 Step 8: append in the new image area;

Java based RXOR:

Step 1: Enter the key value.

Step 2: Key value will match on the fly mechanism.
 Step 3: Consider the substring value with the same pixel form starting to the final length.
 Step 4: Make an object for the above substring;
 Step 5: Pass it in terms of object.
 Step 6: Loop is considered in row and column
 For $j=length-1$ to 0.
 Find the substring.
 The above procedure will be parsing up to 0.
 Step 7: Finally Image will be appended based on height width specified.
 Step 8: append in the new image area;
 At that point we compute the histogram to demonstrate the contortion in the first picture, XOR picture and Encrypted Image. A photo histogram is a graphical proclamation of the greatness of pixels in a statue as a stage of their articulation. Histograms are required all over of receptacles, on in each heading events nose speaking to a Specific complement as needs be yard.

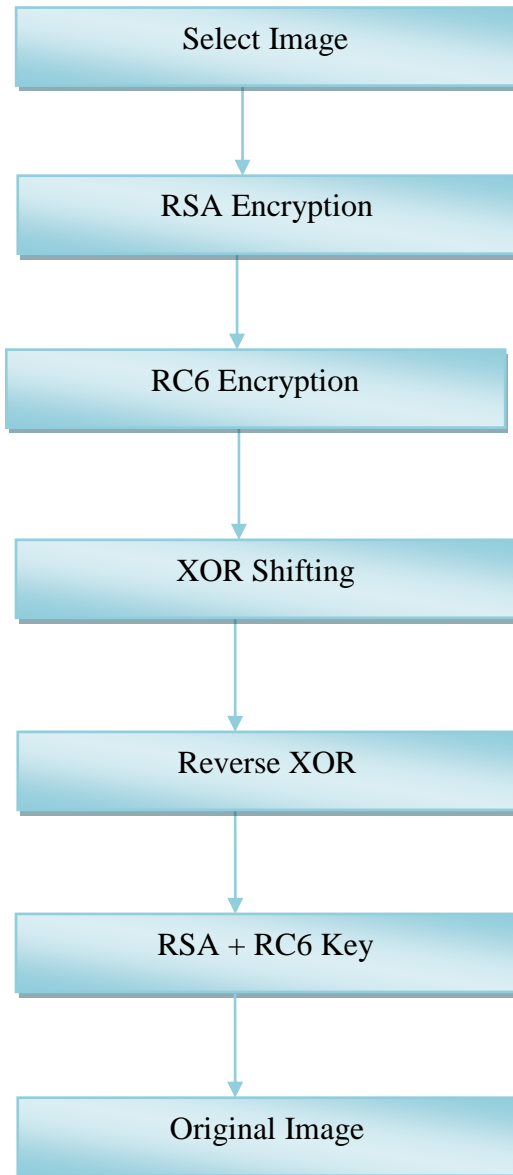


Figure 1: Flowchart

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 different images. First we have applied RSA and 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. Figure 3 to 5 shows the bin calculation. 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 it is shown in table 1 and 2 it is higher with less difference. We have also calculated the information entropy to check the loss in information when cryptography is performed. The results in table 2 show very less difference which shows less information loss by our approach.

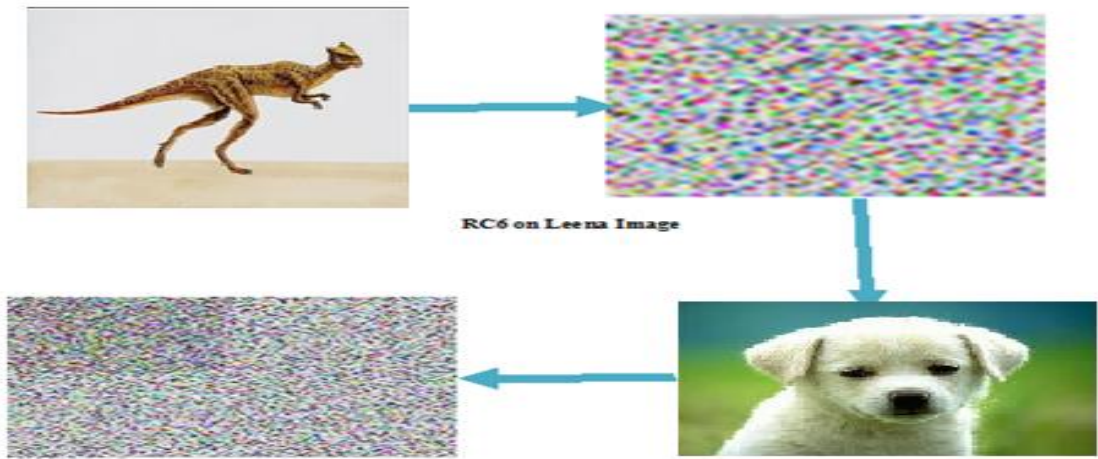


Figure 2: RSA + RC6 + XOR on Image

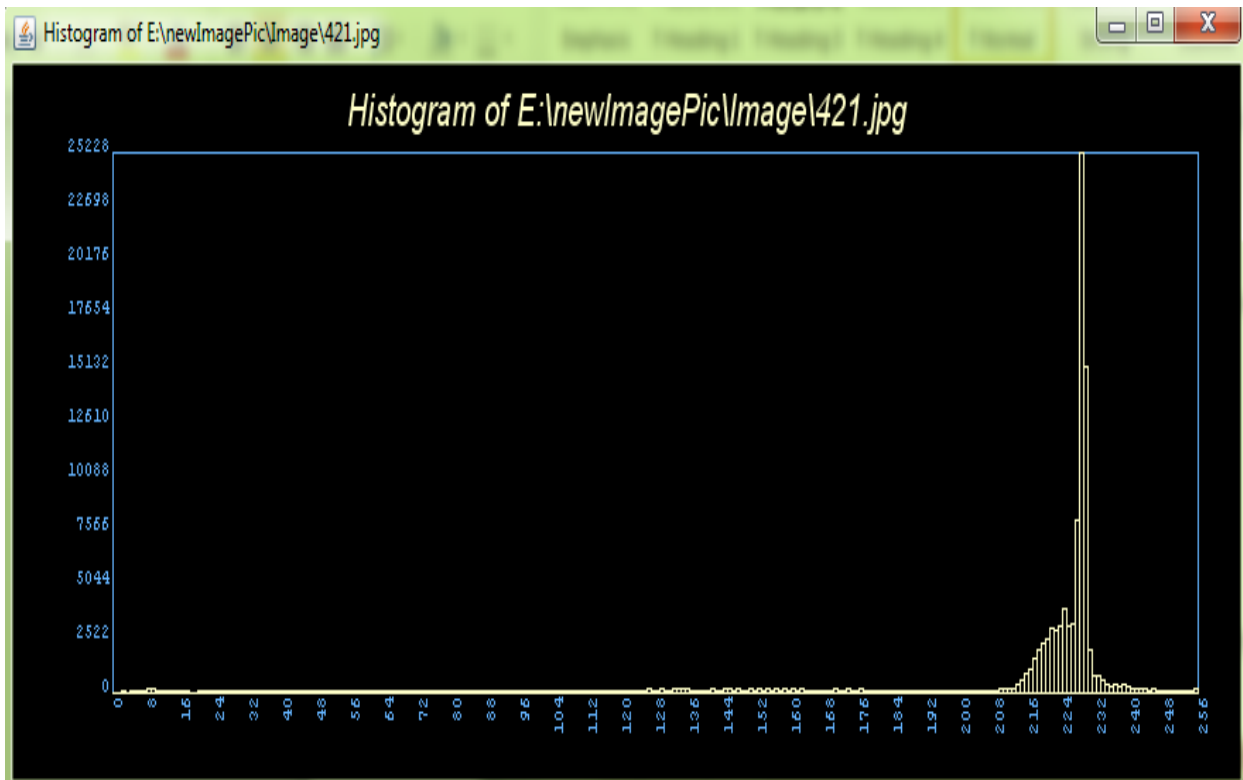


Figure 3: Original Image Histogram of Image

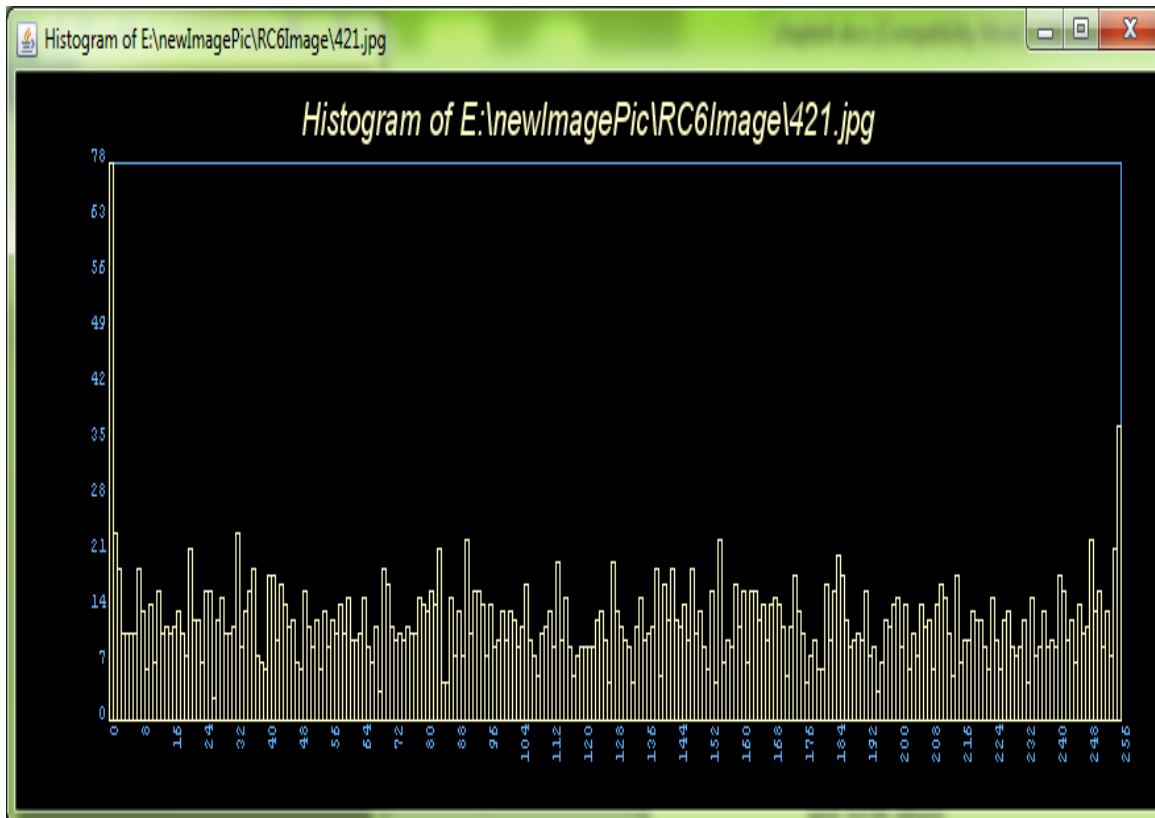


Figure 4: Image Histogram of Image after applying RSA and RC6

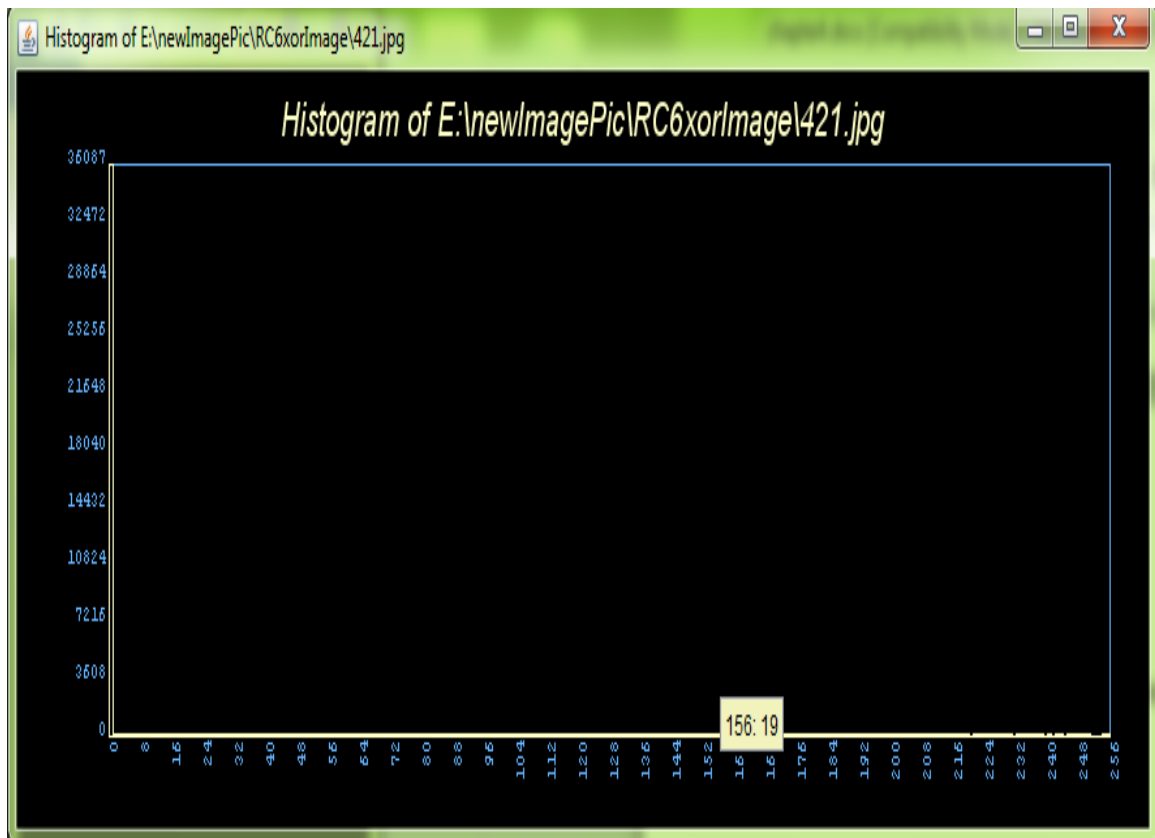


Figure 5: Image Histogram of Image after applying XOR

Image	Methods	Linear Corelation	Normalized Corelation	Corelation Coefficient
Babrasmall	Original	52273.25	1	1
	Encrypted	50532.106	0.96	0.663
	XOR	55952.65	0.98	0.70
Cameraman	Original	56939.08	1	1
	Encrypted	55952.65	0.98	0.70
	XOR	57446.90	0.973	0.488
914	Original	50925.49	1	0.38
	Encrypted	49146.94	0.96	0.66
	XOR	52468.58	0.965	0.380
513	Original	46400.29	1	1
	Encrypted	44046.42	0.94	0.624
	XOR	48093.07	0.933	0.362

Table 1: Correlation Analysis

Image Name	Entropy for Original Image	Entropy for Encrytpd Image	Difference
Babrasmall	7.95	7.98	0.03
Cameraman Image	7.90	7.98	0.08
914	7.97	7.99	0.02
513	7.97	7.98	0.01
Leena Image	7.93	7.98	0.05

Table 2: Information Entropy (Image Size 256 *256)

5. Conclusion

This paper provides a security framework for image database. The image encryption is applied by RSA and RC6. RSA and RC6 is used and also enable key and size variability so the security is improved. Then XOR is applied 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.

References

- [1] A. Mitra, Y V. Subba Rao, and S. R. M. Prasanna, "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," *Journal 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. Wao, 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 , " Chaos - 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] 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.
- [34] Apoorva Shrivastava and Lokesh Singh, " A New Hybrid Encryption and Stenography Technique: A Survey ", International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-3, Issue-14, January-2016, pp.8-13.
- [35] Priyank Singhai and Amit Shrivastava, " An efficient Image Security mechanism based on Advanced Encryption Standard " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-13, December-2015 ,pp.175-182.
- [36] Prakash Deshmukh, Yogesh Rai and Santosh Kushwaha, " Identifying Malicious Behavior in MANET: A Survey " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-4, March-2015 ,pp.43-48.
- [37] Zaher, Ashraf A. "A cryptography algorithm for transmitting multimedia data using quadruple-state CSK." Computer, Communications, and Control Technology (I4CT), 2015 International Conference on. IEEE, 2015.
- [38] Kharat, Pradeep H., and S. S. Shriramwar. "A secured Transmission of data using 3D chaotic map encryption and data hiding technique." Industrial Instrumentation and Control (ICIC), 2015 International Conference on. IEEE, 2015.
- [39] Hamiche, Hamid, et al. "Secure data transmission scheme based on fractional-order discrete chaotic system." Control, Engineering & Information Technology (CEIT), 2015 3rd International Conference on. IEEE, 2015.
- [40] Sathishkumar, G. A., Srinivas Ramachandran, and K. Bhoopathy Bagan. "Image encryption using random pixel permutation by chaotic mapping." In Computers & Informatics (ISCI), 2012 IEEE Symposium on, pp. 247-251. IEEE, 2012.
- [41] Mohammad Ashiqur Rahman and Ehab Al-Shaer, "A Formal Approach for Network Security Management Based on Qualitative Risk Analysis", IEEE 2013.
- [42] S. P. Metkar and M. V. Lichade, "Digital image security improvement by integrating watermarking and encryption technique," Signal Processing, Computing and Control (ISPCC), 2013 IEEE International Conference on, Solan, 2013, pp. 1-6.
- [43] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," Image Information Processing (ICIIP), 2013 IEEE Second International Conference on, Shimla, 2013, pp. 607-611.