Two Layer Image Encryption using Symmetric Key Algorithms

Sumakshi Chauhan, Shreya Pathak, Sumit Kumar

***Abstract:** Security of data (text, audio, and images) is becoming more complex with the increment in its amount. In order to upsurge the reliability, the captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) is used to ensure authenticity. In contrast, even these captchas can be hacked and security can be easily impeached, aim of these captchas is to identify if the user is genuine or else if it is just a robot trying to spam the system. This paper presents auxiliary hybridization of AES and Blowfish cryptographic algorithms for image encipherment and decipherment. Here, AES is using Blowfish as its subroutine where Blowfish encrypts and decrypts the AES encoded image. This is then handed to AES for second level decryption. Here the image which is to be encrypted is applied to AES algorithm, its output is further used as an input for Blowfish algorithm. Output of this doubly encrypted image is then decrypted in the reverse order of encipherment. This auxiliary hybridization adds security to the image rendering it the capacity to become useful in highly important organizations. Private key cryptography uses single secret key at both, the sender and the receiver end. Using symmetric key cryptographic algorithm for this process makes the complete process fast and more secure in comparison to when asymmetric cryptographic algorithms are used for the same purpose. Moreover, symmetric key cryptographic algorithms are more suitable for larger files and images. These also help in maintaining the confidentiality of the data.**

***Keywords:** AES Algorithm, Auxiliary Hybridization, Block Cipher, Blowfish Algorithm, Captcha Security, Symmetric Cryptography*

I. INTRODUCTION

Security of data plays a very vital role while transmitting over a network that is not trustworthy. So these data need to be secured before transmission. To secure these data we convert the data into a code also known as a cipher, and we call this process as encryption. At the receiver side cipher data needs to be decrypted with the help of right key. This technique is used to prevent an unauthorized user from accessing the original message. Decrypting cipher along with the suitable key is the only way to retrieving the real image/message.

Revised Manuscript Received on May 30, 2020.
* Correspondence Author

Sumakshi Chauhan*, Information Technology, ABES Institute of Technology, Ghaziabad, India. Email: sumakshichauhan@gmail.com
Shreya Pathak, Information Technology, ABES Institute of Technology, Ghaziabad, India. Email: pathak97shreya@gmail.com
Sumit Kumar, Information Technology, ABES Institute of Technology, Ghaziabad, India. Email: sumit.kumar@abesit.in

A. Description of AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key algorithm which works on data blocks of size 128 bits and has three different cipher key lengths 128,192 or 256 bits. The number of rounds of the algorithm is 10, 12, or 14 which will depend completely on the key length used. At the beginning of the Rijndael's block cipher subset, the original image is used as an initialization vector to state matrix while the input master key is used as an initialization vector to the key matrix.

The AES module of our system will consist of 14 rounds the output will be produced through processing two matrices independently in each round and at last their outputs are combined at the end of each round in the Add Round Key phase. The number of execution round of the AES algorithm depends upon the cipher key length which is shown with the help of the table given below

Table-1: Rounds of AES algorithm

Key length	128	192	256
No of rounds	10	12	14

The encipherment process of AES algorithm consists of four different rounds which are parts of the round function that comprises of four different byte-oriented transformation these rounds are governed by the following four stages:

- Substitute Byte
- Shift Rows
- Mix Columns
- Add round key

While during decoding we will use the opposite procedure of encoding that comprises of below four stages:

- Inverse shift row
- Inverse substitution byte
- Add round key
- Inverse mix column

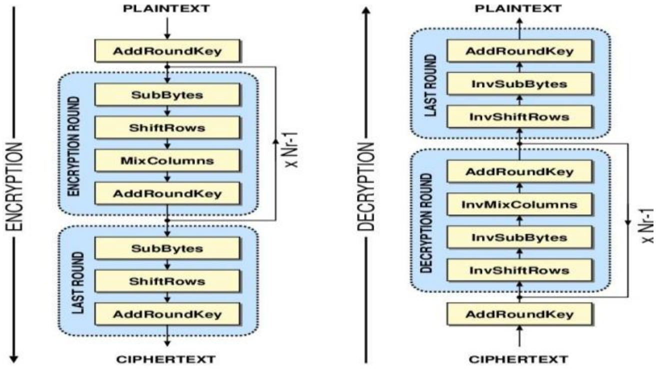

Fig. 1: Encryption and Decryption process of AES algorithm

B. Description of Blowfish Algorithm

Blowfish algorithm can be efficiently utilized for hardware implementation. It consists of a lookup table, addition, and XOR. Furthermore, it has a fiestal structure with 64-bit block size and has a variable length key. Along with this blowfish algorithm is a 16 round process and uses expansive key subordinate S- boxes. Blowfish structure resembles a CAST-128, which uses rigid and static S-boxes. The whole 64 bit data is divided into two segments of 32 bits and processed separately as shown in Figure2.

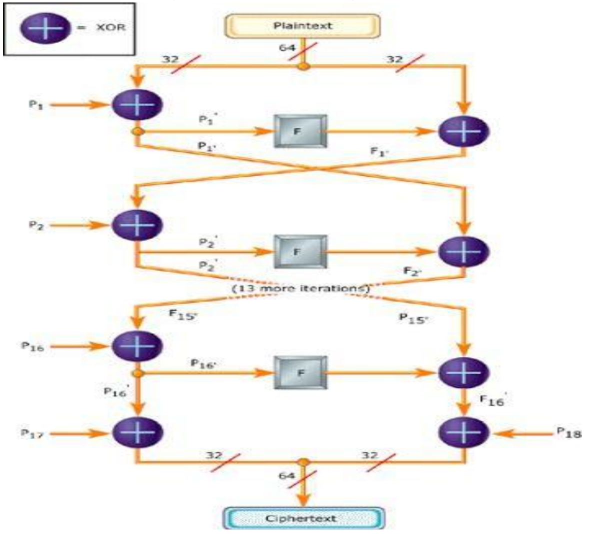

Fig. 2 : Encryption process of Blowfish algorithm

II. LITERATURE REVIEW

Noor Kareem Jumaa (N K Jumma, 2018) In this paper the problem of secret key exchanging with the communicated parities had been solved by using a random number generator which based on Linear Feedback Shift Register (LFSR). The encryption/decryption is based on Advance Encryption Standard (AES) with the random key generator. Also, in this paper, both grayscale and colored RGB images have been encrypted/decrypted. The functionality of proposed system of this paper, focuses on three features: First feature, is dealing with the obstetrics of truly random and secure encryption key while the second one deals with encrypting the plain or secret image using AES algorithm and the third concern is the extraction the real picture through decryption. “Mean Square Error (MSE)”, “Peak Signal to Noise Ratio (PSNR)”, “Normalized Correlation (NK)”, and “Normalized Absolute Error (NAE)” are measured for both (original-encrypted) images and (original-decrypted) image to study and analyze the performance of the recommended system according to image quality features.

Priya Deshmukh (P Deshmukh, 2016) With the assistance of MATLAB coding usage of an AES algorithm is incorporated and re-enacted for picture encryption and decryption. This framework scrambles and decodes the picture with the goal that it can't be gotten to an unapproved individual during transmission on the system.

Sneha Ghoradkar and Aparna Shinde (S Ghoradkar, A Shinde 2015) proposed a system that will use AES algorithm for encoding and decoding, which has block size equivalent to 128 bits and key size of 256 bits. Total rounds for 256 bit key size is 14. In this system the original image will act as input for AES encryption algorithm and encrypted image will act as input for AES decryption algorithm to get original image.Shraddha more and Rajesh Bansode (S More, R Bansode
2015) implemented an efficient AES 128-bit algorithm. It performs 10 rounds of the given function in order to analyze the efficiency. This execution presented an attack on AES software implementation. Also, this method has reduced the time complexity in comparison to the current one. Also, it thinks about the time taken for AES encryption and the unscrambling process for a wide range of data. The paper likewise displays a side-channel attack on the standard AES usage.

T. Venkat Narayana Rao, V. Rishitha Reddy and Kapa Vinutha (T. VN Rao, V. R Reddy, and K Vinutha) used blowfish algorithm for secure encipherment and decipherment of images. Blowfish resists illegal attacks and works much faster and more efficiently than the other algorithms. Here, bits of the primary image is split into the number of the blocks. Then with the help of a key and encryption algorithm, the initial image is encrypted which is not visible to anyone. Finally, the encoded image is decoded with the same key which was used for encoding process.

Pia Singh and Karamjeet Singh (P Singh, K Singh, 2013) This paper renders security to images with the help of a secret-key. It uses a block cipher in order to improve algorithm’s performance. Feistel network employed in blowfish enables it to run faster in comparison to other symmetric-key cryptographic algorithms. The suggested work is described utilizing MATLAB. The future work based on this paper could be increased no of rounds so that attackers cannot easily break the algorithm as Blowfish is unbreakable till an attacker tries 28x+1 combination where x is the number of rounds.

III. PROPOSED TECHNIQUE

The algorithm explained in this paper is able to add a second security layer so as to complex the process of data hacking using image recognition. This algorithm can be used to enhance security of an image. In the current scenario, the captcha is generated to check if the access is done by a human and not by a robot. However, the captcha can be hacked using image recognition techniques. Therefore, the algorithm presented in this paper will help to add a security layer to the captcha. Consequently, this will ensure the integrity of the captcha.

Firstly, image is encrypted using AES algorithm, this results into an intermediate cipher data. Then this
intermediate cipher data will again be encrypted with the second algorithm which is Blowfish and final cipher data will be obtained. Thus, the final cipher data obtained will be decrypted using Blowfish and AES. Complete process can be understood from Figure3:

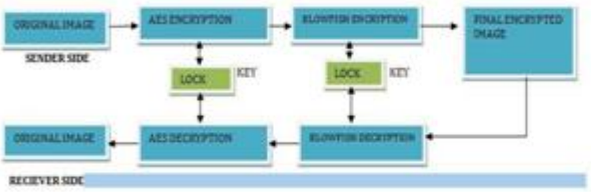

Fig. 3: Complete process of image encryption and decryption with 2-layer security

IV.PROPOSED ALGORITHM

Step 1: Encrypt the input image (original) using AES algorithm
Step 2: Encrypt the intermediate cipher using Blowfish algorithm
Step 3: Obtain the final cipher data.
Step 4: Decrypt the final cipher using Blowfish algorithm
Step 5: Decrypt the intermediate cipher using AES algorithm

Step 6: Obtain the original image.

V. RESULT AND DISCUSSION

AES has a substitution-permutation/non-fiestal structure. Its time complexity is O (1) in general cases. On the other hand, Blowfish has a Feistel structure with high flexibility. Also, it renders high data security without any backdoor vulnerability (Z Hercigonja). Below is the table which compares time complexity of AES (Rijndael) and its variants along with the Blowfish algorithm.
Initially, picture is encoded with the aid of Rijndael's block cipher subset. It is used as first algorithm because it has no weak keys. Thus, it protects from linear, differential cryptanalytics and interpolation attacks.

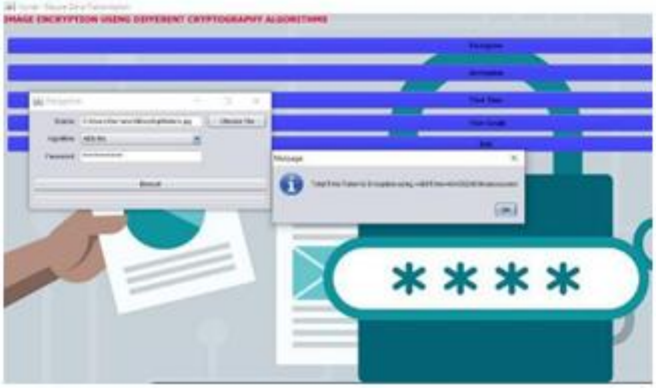

Fig.4: Encrypted an Image named Nature.jpg using AES algorithm

Now encrypting this AES encrypted image through Blowfish Algorithm

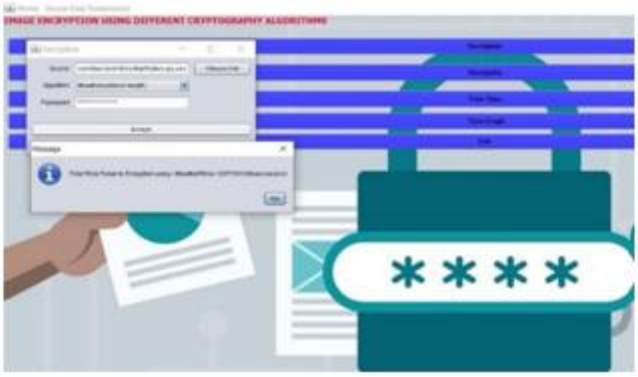

Fig. 5: Encrypting Nature.jpg.aes image with Blowfish Algorithm

Thus, the image is doubly encrypted now. Now decrypting this 2-layer encrypted image in a reverse order of encryption

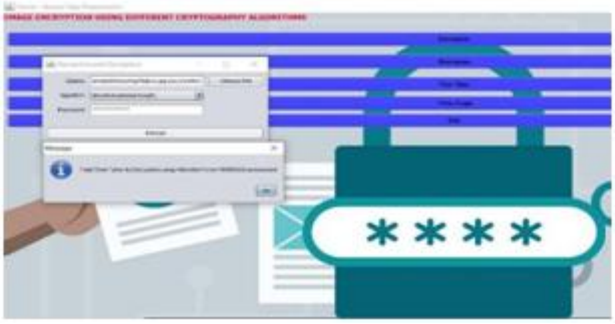

Fig. 6: Decrypting the above doubly encrypted image using Blowfish Algorithm

So, the decrypted image is again decrypted using the AES algorithm

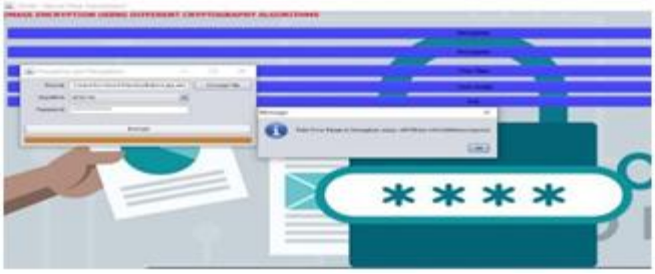

Fig. 7: Decrypting the above decrypted image further using AES Algorithm

Therefore, the overall time for double layer encryption and decryption is shown below (Note the time shown is in nanoseconds):

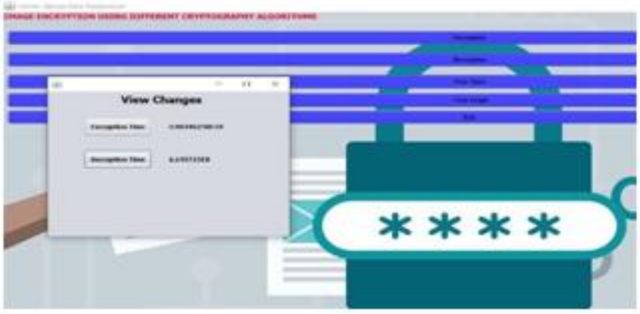

Fig. 8: Overall Encryption and Decryption Time

VI.CONCLUSION

To recapitulate the above discussion, this research reveals that the hybridization of non-Feistel and Feistel structures further improves image security. This auxiliary hybridization acts as 2-layer security for an image. It shows how double-layer encryption intensifies security. This algorithm can be implemented to secure captcha images. Furthermore, it can be adopted to the banking sector and other organizations where image security is a major concern. Though the introduction of no Captcha by Google has solved a major problem of image security, sectors with highly crucial data still use the combination of reCaptcha and noCaptcha. Thus, this algorithm fits perfectly for the above-mentioned organizations and sectors which uses the above combination for encryption. It uses the amalgamation of fiestal and non- fiestal structures.

As discussed initially, this study is based on the qualitative analysis of implementing two layer cryptographic algorithm, hence it should be considered only as a means not as an end while formulating and implementing any security-related measures. Other quantitative factors like time and space complexity also need to be taken into consideration before the implementation of this algorithm. This research is a small step towards using multiple cryptographic algorithms in advancing the existing image security, strengthening from the known vulnerabilities and serves as a foundation for further research in this space.

REFERENCES

1. Ali Abdulgader, Mahamod Ismail, Nasharuddin Zainal, Tarik Idbeaa "enhancement of AES algorithm based on chaotic maps and shift operation for image encryption", Journal of Theoretical and Applied Information Technology 10th January 2015. Vol.71.
2. Aloha Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I8 (2203),229-234.
3. Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.
4. Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).
5. Ayushi Arya "effective AES implementation" International Journal of Electronics and Communication Engineering & Technology (IJECET) Volume 7, Issue 1, Jan-Feb 2016, pp. 01-09, Article ID: IJECET_07_01_001.
6. Cryptography www.cryptographyworld.com/concept.html (URL valid as on 11 April 2020)
7. Gebze and Kocaeli, 2005, "Analysis and Comparison of Image Encryption Algorithms".
8. Ismail Amr Ismail, et.al," A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.
9. K. Kanagalakshm, M. Mekala "Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key", International Journal of Computer Applications (0975 – 8887) Volume 146 – No.5, July 2016.
10. Kaladharan N, Unique Key Using Encryption and Decryption of Image, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014.
11. L. Scripcariu and M. D. Frunză, "Modified Advanced Encryption Standard," vol. 3, no. 23, pp. 23–26, 2012.
12. Monika Agrawal and Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877- 882.
13. Mustafa emad hameed, Masrullizam Mat Ibrahim, Nurulfajar Abd Manap,"Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security", Journal of Telecommunication Electronic and Computer Engineering ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. 10 No. 1
14. Noor kareem jumaa "Digital Image Encryption using AES and Random Number generator",Iraqi Journal of Electrical and Electronic Engineering Volume 14, No. 1- 2018.
15. Pia singh, Prof. Karamjeet singh "Image Encryption And Decryption Using Blowfish Algorithm In Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 ISSN 2229-5518.
16. Priya Deshmukh "An image encryption and decryption", International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518.
17. Roshni padate and Aamna patel. Image Encryption and Decryption Using AES Algorithm. International Journal of Electronics and Communication Engineering & Technology, 6(1), 2015, pp. 23 -29.
18. S. S. sudha, S. divya "Cryptography in Image Using Blowfish Algorithm", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 Impact Factor (2013): 4.438.
19. Shraddha more and Rajesh bansode "Implementation of AES with Time Complexity Measurement for Various Input", Global Journal of Computer Science and Technology: E Network, Web & Security Volume 15 Issue 4 Version 1.0 Year 2015.
20. Sneha ghoradkar and Aparna shinde "Review on Image Encryption and Decryption using AES Algorithm", International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015)
21. T. Venkat narayana rao, V. Rishitha reddy and Kapa vinutha "Secured Image Encryption and Decryption Using Blowfish Algorithm", International Journal on Future Revolution in Computer Science & Communication Engineering ISSN: 2454-4248 Volume: 5 Issue: 4.
22. Tingyuan nie and Teng zhang, "A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.
23. Wikipedia "https://en.wikipedia.org/wiki/Blowfish_(cipher)"(URL valid as on 11 April 2020).
24. https://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/ (Abdel-Karim Al Tamimi ; URL valid as on 11 April 2020)
25. Z hercigonja, "Comparative Analysis of Cryptographic Algorithms", International Journal of Digital Technology & Economy, Vol. 1 No. 2, 2016.

AUTHORS PROFILE

Sumakshi Chauhan is a final year student pursuing B. Tech from Information Technology branch at ABES Institute of Technology, Ghaziabad. She is an avid programmer and loves to explore new horizons in the field of Cryptography and Machine Learning. She has received multiple appreciations from the Government of India for the effective solutions and contribution through innovative ideas.

Shreya Pathak is a final year student pursuing B. Tech from Information Technology branch at ABES Institute of Technology, Ghaziabad. She loves solving problems based on real life and come with optimized solution each time. Her field of interest includes cryptography and networking. She loves to explore new technologies and languages.

Sumit Kumar is currently working as Ph.D. Scholar in Uttarakhand Technical University, Dehradun, India. He has over 13 years of experience with leading Institutions. He has published more than 10 research papers in reputed journals and international conferences. His research interest area is Finite State Testing of Graphical User Interface. He has received Excellence Award for Best Teaching and Learning Practices (April-2012) by Prof S K Kak (Vice Chancellor MTU).

Retrieval Number: G5285059720/2020©BEIESP
DOI: 10.35940/ijitee.G5285.059720
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication