IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 4 ISSUE : 11 Print / Issue Publication Date: 10-May-2020

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2020.v04i11.066

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 375-377
Published Online March 2020 in IJEAST (http://www.ijeast.com)

SYMMETRIC KEY DESIGN FOR IMAGE ENCRYPTION USING FUNCTION

Agnes Ahalya.A
Department of CSE
Loyola-ICAM College of Engineering and Technology, Chennai

Janet Siliya.J
Department of CSE
Loyola-ICAM College of Engineering and Technology, Chennai

***Abstract*—This study shows the design of a new symmetric key design using mathematical function and string that can be used for image encryption. The input is an image and a mathematical function that is generated from a string (text). The symmetric key must be shared through the secure channel.**

Keywords—**symmetric key, mathematical function, string, image encryption, secure channel.**

I. INTRODUCTION

Private key cryptography consists of symmetric keys that are shared between one or more authorized users. In private key cryptography, the shared key is used for encryption of plaintext and similarly for the decryption of ciphertext. Algorithms like Vignere, Vernam, DES and other similar ones have been using text, S-Boxes, numbers as their shared key. The algorithm uses a composite key generated from a function and image. The algorithm is fully a transformation algorithm.

II. PROPOSED ALGORITHM

A. Encryption process

The image to be secured or protected is read as byte array represented as [M1,M2,…, MN]. The text key is read from the sender.The string literals of the test are converted into ASCII value[X1, X2,…, Xl]. The constant for the function is decided based on user-defined logic. The logic used here c is equal to the scaling factor of the secret image after encryption.
Then it undergoes

$$f(x)=x+c$$
$$g_1(x)=mx+c$$
$$f_e=g_1.f$$
$$f_e=(m*x)+((m+1)*c$$

where ‘x’ accepts value from [X1, X2,…, Xl] in cyclic order and ‘m’ from [M1,M2,…, MN] in cyclic order

Fig. 1. Original secret image

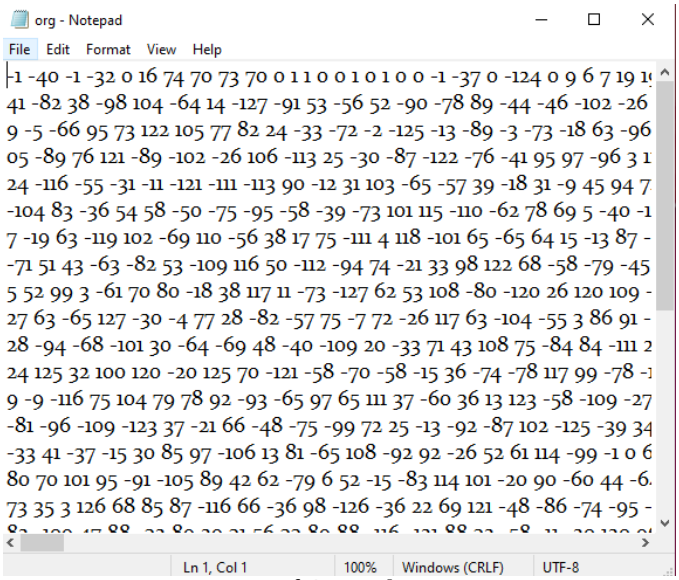

Fig. 2. Bytes of Original secret image

There is a possibility that ‘mx’ may acquire a value greater 127 or less than -128 and so 16 bits may be required for its storage. This causes expansion of the image. This complicates the process of cryptanalysis on the encrypted image thereby enhancing the security.The encrypted image is then sent through a secure channel to the receiver.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 375-377
Published Online March 2020 in IJEAST (http://www.ijeast.com)

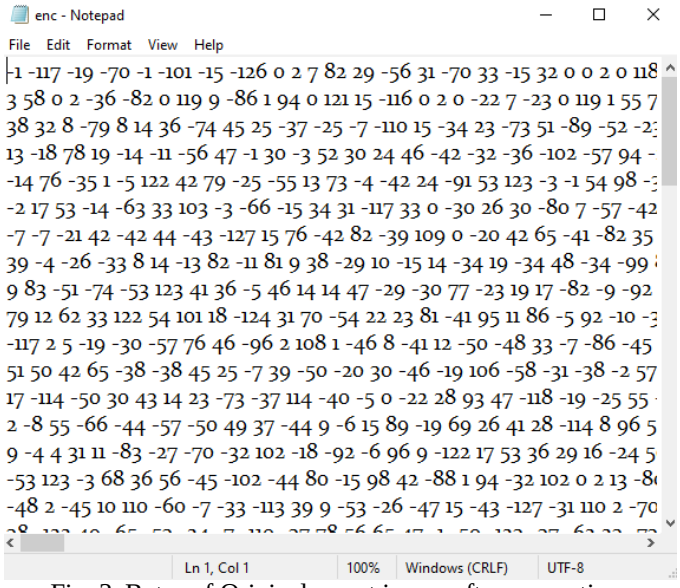

Fig. 3. Bytes of Original secret image after encryption

B. Decryption process

The encrypted image is read as byte array represented as [E1, E2,…, E2N]. The shared text key is read from the receiver. The string literals of the test are converted into ASCII value[X1, X2,…, Xl]. The constant for the function is decided based on user-defined logic. The logic used here c is equal to the scaling factor of the secret image after encryption. There is a possibility that 'mx' may acquire a value greater 127 or less than -128 and so 16 bits may be required for its storage. The expanded image must be contracted. The original image size is obtained by dividing the encrypted image size with the scaling factor.

Then it undergoes

$$f(x)=x+c$$
$$g_2(x)=m(x+c)$$
$$f_d=g_2.f$$

To extract [M1, M2,…, MN] apply

$$m = f^{-1}([e]/(x+c))$$

where 'x' accepts a value from [X1, X2,…, Xl] in cyclic order and 'e' from [E1, E2,…, EN] in cyclic order and m is written to [M1, M2,…, MN].[M1, M2,…, MN] is stored as decrypted image.

III. Experiment and Result

A. Accuracy

Accuracy is the calculation of correlation between the original image and the decrypted image. Correlation coefficient pattern of the images is generated and compared.

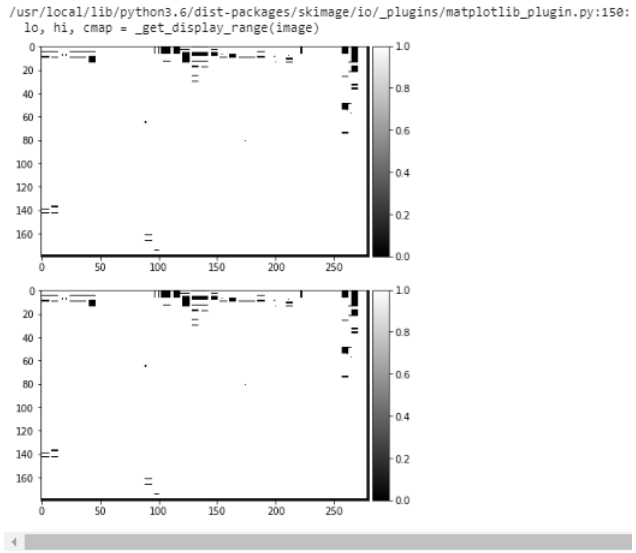

Fig. 4. Correlation pattern of original image vs decrypted image

B. Avalanche

The avalanche effect is the desirable property where if the input is changed lightly the output show variations significantly.

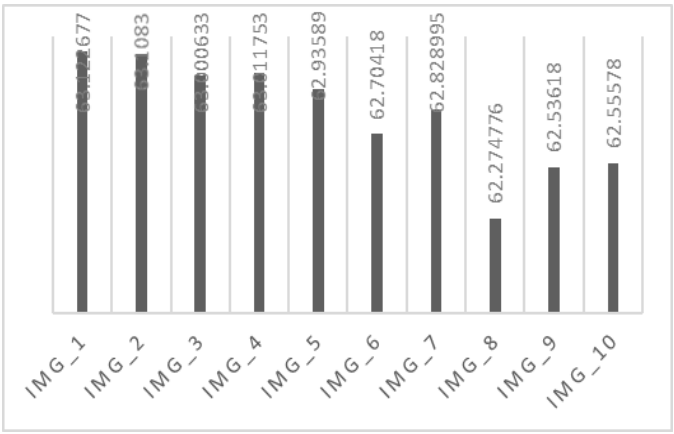

Fig. 5. Graph representing the avalanche percentage for 10 different images

C. Variation

The variation between the original image and encrypted image is an important favourable property in any cryptography. When the percentage of variation is more it becomes more to perform cryptanalysis.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 375-377
Published Online March 2020 in IJEAST (http://www.ijeast.com)

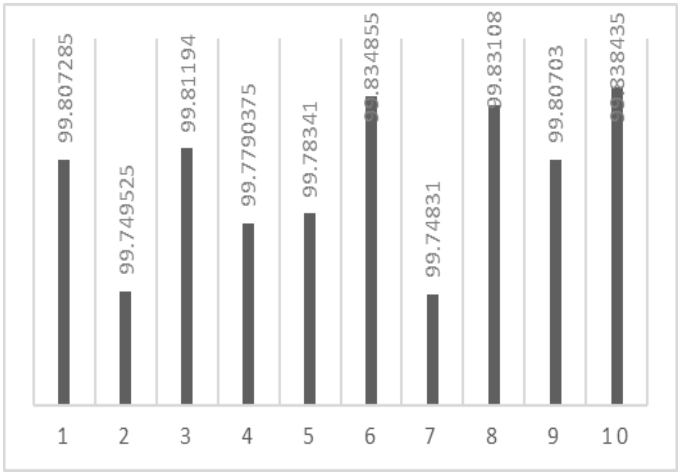

Fig. 6. Graph representing the percentage of variation

IV. CONCLUSION

The symmetric key mechanism has been proposed and been tested. The encryption process and decryption process of the image with text and function is done and tested. The accuracy has been tested and results obtained were favourable.

V. ACKNOWLEDGMENT

We like to thank Loyola-ICAM College of Engineering and Technology for their constant support and we would also like to extend our gratitude to Santa Maria Matric. Hr. School for allowing us to test this public key design as part of the ICE algorithm on their official website.

VI. REFERENCE

[1] Naveen Chandra Gowda, P. Sai Venkata Srivastav, Guru Prashanth.R, Raunak.A, Madhu Priya R, (2019). "Steg Crypt (Encryption using steganography)", pp(224-229).
[2] Madhu Sudan, Vipul sharma, (2015). "Two New Approaches for Image Steganography Using Cryptography", pp(202-207).
[3] Abdelkader Moumen and Hocine Sissaoui, (2017). "Images Encryption Method using Steganographic LSB Method, AES and RSA algorithm".
[4] Radha S. Phadte, Rachel Dhanaraj, (2017). "Enhanced Security with Steganography and Cryptography" pp(11-16).
[5] Nath, Asoke & Roy, Sayudh & Gopalika, Chahat & Mitra, Debayan, (2017). " Image Steganography using Encrypted Message ", pp(7-11).
[6] Sahil Lotlikar , Ashish Gupta , Jayesh Thorat , Sandhya, (2017). " Image Steganography and Cryptography Using Three Level Password Security", pp(1371-1374).
[7] Arshiya Sajid Ansari ,Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez .I. J. , (2019)." A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", pp(11-25).

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143