International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Conglomerate Encipher

B. Karthikeyan, R. Phani Teja, G. V. Gowtham

Abstract*: As the technology is growing day by day, the entire human activities are dependent on it, thereby the rate of transfer of data is increasing exponentially. The knowledge discovered from this data can be in the form of graphs, plots, images etc. Due to the loop holes in the technology, the attackers can retrieve the data which increases the rate of Cyber-crime. In this evolved world, images are playing a vital role in transmitting information. There is a need to implement few efficient protective schemes that provides higher security. In this paper one such protective scheme is proposed using Huffman code and AES mechanism. Firstly, the plain text is taken and encoded with Huffman code then the output obtained after encoding will be given as an input to the AES which results in the encrypted data. The encrypted data will be hidden into an image. Each character consists of 8 bits which are hidden in Grey image. After hiding this encrypted data into the grey image the original pixels of the image will be disturbed. In this paper we will calculate the (MSE) and (PSNR) between the original image and output image. The problem that might occur during this process is the output obtained from the Huffman code may not always produce 128-bit because AES need 128 bit as input to provide optimal solution.

***Index Terms*: AES, Huffman Code, MSE, PSNR**

I. INTRODUCTION

In the modern communication system, the Network security is playing a vital role. To protect against the unauthorized access, to provide the integrity of data and to sustain the confidentiality the essence of network security was risen. The cryptography and Steganography are two different views in network security where cryptography is based on the encryption of message while the steganography deals with hiding the traces of communication. The another key difference between the cryptography and the steganography is that in the steganography the change in structure of message is not accomplished while in the cryptography the secret message structure is altered. The steganography is implemented on video, audio, text, image whereas the cryptography is implemented only on text files. In [1], the goal of cryptography is data protection whereas the goal of the steganography is secret communication. This paper completely deals with the techniques involved in Steganography. The technique of communication hiding by masking the secret message into fake message is called as "STEGANOGRAPHY". The steganography's secrecy is dependent on the data encoding system's secrecy. In this paper the encoding systems used are Huffman code and AES algorithm.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
B.Karthikeyan, School of Computing, SASTRA Deemed to be University, Thanjavur , India.
R. Phani Teja, Information Technology, School of Computing SASTRA Deemed to be University, Thanjavur, India.
G.V.Gowtham, Information Technology, School of Computing, SASTRA Deemed to be University, Thanjavur, India.

II. LITERATURESURVEY

When compared to conventional Binary Search Tree, the compressed Huff-man decoding method is more efficient. In [1] the algorithm converts the initial Huffman tree to recursion Huffman tree and uses the numerical interpolation to speed the decoding process .By the usage of recursion Huffman tree procedure the decoding of more than a symbol at a particular time is increased.

When the data is sent via unsecured channel it should be encrypted and compressed, Generally after encryption of data and compressing using many algorithms is not advisable because the decryption is impossible in those cases. In [2] the data is encrypted and compressed by the usage of quantization mechanism and Huffman coding.

The usage of multiple Huffman tables has been increased and there is need to secure the content in it. In order to protect the content of data the encryption of data with speed should be necessary. In [3] the data is encrypted with an algorithm that is faster than AES (advanced encryption standard).

The transmission of data is sensitive to attacks if it is sent by electric ways. In order to safeguard the information the security plays a key role. In [4] the AES is improved by enhanced security. The main factor in AES lies in s-box operations. These changes gives an enhancement in encryption when compared classic AES by the usage of sequence repeater.

AES is best encryption algorithm till today. But, the occurrence of faults reduces its factors and causes the information leakage. In [5] a fault detection process for reliable AES has been used by the modification of AES architecture.

The Cryptography based algorithms mainly present to safeguard private data from other users but these are vulnerable to noise. In AES the difference in one bit leads to very great damage in decrypted data. In [6] it removes the noise based on some measures. These measures are the mean variance method (MLVM), global variance method (GVM).

Usage of quaternary tree speeds up the decoding time of Huffman codes than the binary tree. While using the variable length binary Huffman code, the balance between speed and memory usage cannot be achieved so easily. The usage of Quaternary tree here results in the most appropriate code word that speeds the way of searching. In [7] the performance of the algorithms with the Huffman-based techniques is analyzed in terms of decoding speed and compression ratio.

The compression of data is done by the most commonly and efficiently used technique, HUFFMAN CODE. Cost of Huffman table can be decreased by new condensed Huffman table.

In [8] on comparing the new condensed Huffman table with the classic Huffman table, other enhanced tables, the improvement is that, the spatial necessity is reduced.
In generation prefix-free codes, a well-known technique is Huffman coding. The Huffman coding is the most efficient algorithm used in the source coding field. It is most commonly used lossless compression technique. In spite of having so many advantages by using Huffman coding there are few limitations that arises. The character that has the high chance of repetitions requires less number of bits whereas the character that has less number of repetitions requires high number of bits. In [9] so the better result can be achieved by using the Double Huffman coding, because in Double of Huffman encoding, output code word of the character should be compressed on binary standard.
To resist the linear or differential attacks, AES was proposed. The AES's cryptographic strength is strongly dependent on the S-Box chosen. The disadvantage of already existed linear architecture in S-box is the setback. In [10] a complete analysis of AES algorithm and risen complexity of nonlinear changes in the architecture of S- box using a new performance scheme. In [10] to provide more protection a biometric scheme is used in both encryption and decryption
The well-known symmetric cryptographic algorithm is AES. To broaden its applications, it is important to develop high performance AES. In [11] discuss about the different implementations and designs of AES algorithm. On comparing the standard AES algorithm with fast implemented AES algorithm, the performance has been increased about 50 times in fast implemented AES. On execution of AES is done using CUDA and GPU in parallel, the performance increases by 18 times when compared to fast implementation of AES.
In [12] a new AES-like design by the usage of S-box gyration for key independent is introduced. This property makes the S-box key-dependent and thereby this makes AES robust. Cipher architecture and the classic AES features the same, without changing the value only S-box is made dependent on the key. The NIST statistical test is used to test the new design. In [12] it is further crypt analyzed with algebraic attack.

III. FORMULA

$MSE = (1/n) * \sum_{i=1}^{n} (y_i - x_i)^2$ *,where n is the total no of points and (y-x) is the error rate and* $(y-x)^2$ *represents the square of the errors.*

$PSNR = 10 * (\log_{10}(R^2 / MSE))$ *where R is the maximum fluctuation in the input image data type .If the input image has double-precision floating-point data type then R=1 else R=255 for single floating point data type.*
MSE=Mean Squared Error,
PSNR=peak Signal Noise Ratio.

IV. HELPFUL HINTS

A. Figures

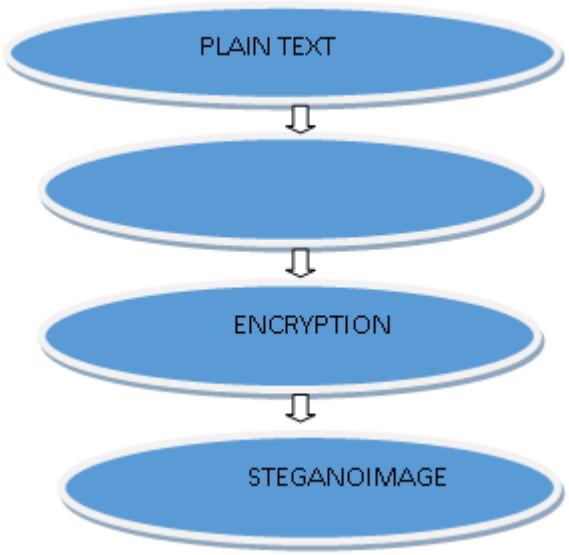


FIG-1: ENCRYPTION PROCESS

In fig-1 initially, the plain text for which the security is provided is Encrypted .Encryption is a process of converting the plain text into Cipher text using a key. But to increase the security of the Plain text it undergoes through a HUFFMAN algorithm to generate a Huffman code. The Huffman code is based on the frequency in the plain text. The output generated by the Huffman code is in the form of Text. The output generated from the Huffman Code will be given as the input to the AES Encryption algorithm. Make sure that the input to the AES Encryption algorithm is 128 bit ,if not divide the text obtained from the Huffman code into 128 bit sized blocks .If the final block is not 128 bit then zeros are padded to make it as 128 bit . The number of zeros padded are considered while decrypting. The output produced by the AES Encryption algorithm will be in form of ones and zeros. The encrypted message will be hidden into an image, this image is known as "STEGANO IMAGE" .Finally this stegano image along with the number of zeros padded is sent to the receiver. Hence the process of encryption is completed here and the process of decryption begins at the Receiver

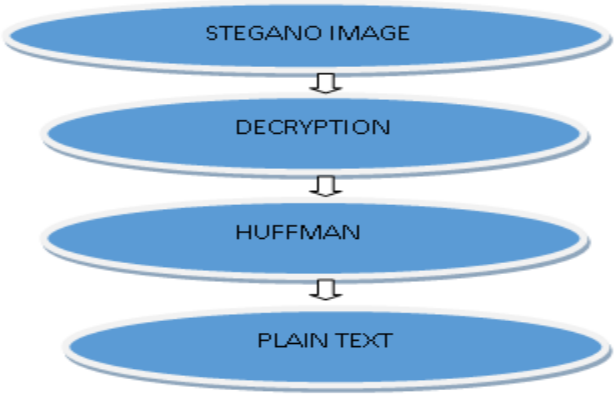


FIG-2: DECRYPTION PROCESS

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

In fig-2 the image and the number of zeros padded will be received at the receiver end will be useful in decrypting the message. The stegano image and the original image will look the same but the pixels will be different .This is because, the message hidden in the image will disturb the pixels of the original image. This difference in pixels between the Stegano image and original image will be used in calculation the MSE, "MEAN SQUARE ERROR". Now using this Stegano image AES decryption algorithm is performed. This AES Decryption algorithm will produce an output in the form of ones and zeros. Before undergoing the process of Inverse-Huffman, the number of zeros padded which is received at the receiver end should be considered in removing the same number of zeros from the output obtained from AES decrypting algorithm. After successful removal of the zeros, this output should undergo "INVERSE-HUFFMAN". The inverse Huffman is used in obtaining the plain text from the output obtained from AES decrypting algorithm. Finally the plain text is obtained as output from the Inverse algorithm. Hence the successful decryption is done.

B. Reference

FIG-3: Reference Image-1

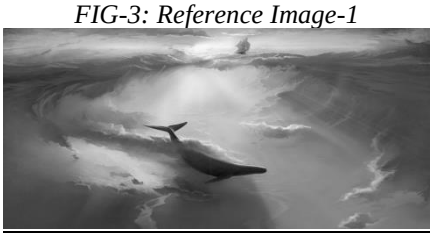


FIG-4: Reference Image-2

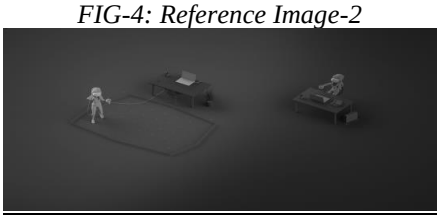


FIG-5:Reference Image-3

C. Table

File Name	Length	MSE	PSNR
100.txt	443	0.122945	57.23369
200.txt	847	0.227329	54.56425
300.txt	1332	0.361629	52.54817
500.txt	2218	0.595657	50.38084
1000.txt	4422	1.183506	47.3991
100.txt	443	0.054811	60.74209
200.txt	847	0.084829	58.84537
300.txt	1332	0.12408	57.19379
500.txt	2218	0.192594	55.28439
1000.txt	4422	0.361712	52.54718
100.txt	443	0.2654	53.8918
200.txt	847	0.306705	53.26359
300.txt	1332	0.370841	52.43893
500.txt	2218	0.465308	51.4534
1000.txt	4422	0.652407	49.98562

D. Equations

*(a)*Encryption Equation:

Let the Plain Text=p;

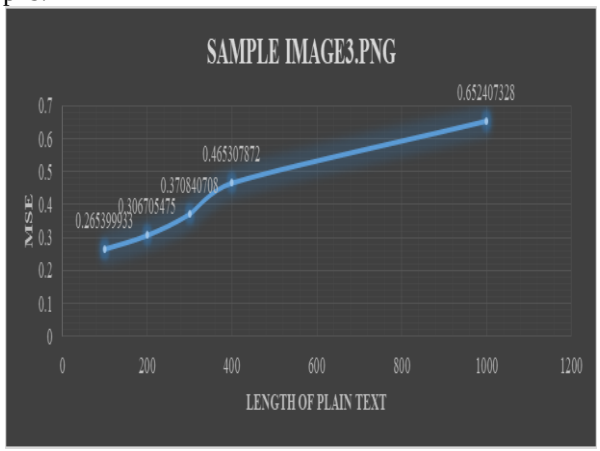
H(p) is the output after obtained after the Huffman encoding function and sent to the encryption and the output is E(H(p)) and the output is Encrypted Huffman Encoded Plain Text.

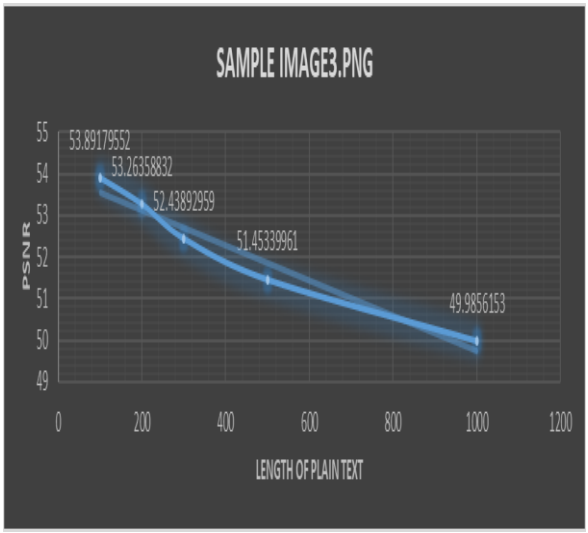
(b)Decryption Equation:

Let the Cipher Text=c;D(c) is the decryption performed on the cipher Text and send to the Inverse Huffman Encoded is IH(D(c)) and the final output is Inverse Huffman Decrypted Cipher Text.

E. Other Recommendations

Graphs:





V. CONCLUSION

Thus the security of the message is increased using the Huffman code and AES Algorithm. The entire process of hiding and retrieving the message into or from the image is done using the grey image. Therefore the main concern on the safeguard of data is achieved by the implementation of Huffman as well as AES. The entire process is less immune to noise when compared to other algorithms that are used to safe the data. The time complexity as well as spatial complexity is also improved.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

REFERENCES

1. A fast algorithm for Huffman decoding based on a recursion Huffman tree" by Yih-Kai Lin, Shu-Chien Huang, Cheng-HsingYang .Published on 2012.
2. Efficient Compression of Secured Images Using Subservient Data and Huffman Coding " by K .S . Kasmeera, Shine P.James, K.SreeKumar. Published on 2016.
3. On the security of multiple Huffman table based encryption " by Qing Zhou, Kwok-Wo Wong
4. Xiaofeng Liao ,Yue Hu. Published in 2011.
5. An efficient AES implementation using FPGA with enhanced security features" by HarshaliZodpe, Ashok Sapkal . Published on 2018
6. A high speed AES design resistant to fault injection attacks" by HassenMestiri, FatmaKahri ,BelgacemBouallegue , Mohsen Machhout. Published in 2016.
7. Denoising and error correction in noisy AES-encrypted images using statistical measures" by Naveed Islam, Zafar Shahid, William Puech. Published in 2015.
8. Balancing decoding speed and memory usage for Huffman codes using quaternary tree" by Ahsan Habib, Mohammad ShahidurRahman . Published in 2017.
9. A Study and Implementation of the Huffman Algorithm Based on Condensed Huffman" by BaoErugude, Li Weisheng, Fan Dongrui, Ma Xiaoyu. Published in 2008 International conference on Computer Science and Software Engineering.
10. Performance comparision of Huffman Coding and Double Huffman Coding" by Rabia Arshad, AdeelSaleem, DanistaKhan . Published in 2016 Sixth International Conference on Innovative Computing Technology(INTECH).
11. A secure software implementation of nonlinear AES S-box with enhancement of biometrics" by Ahsan Habib, Mohammad ShahidurRahman . Published in 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET).
12. Different Implementations of AES Cryptographic Algorithm" by Guang-liangGuo, QuanQian, Rui Zhang. Published in : 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems.
13. A proposal for improving AES S-box with rotation and key-dependent" by Julia Juremi, RamlanMahmod, SalasiahSulaiman. Published in : Proceedings Title: 2012 International Conference on Cyber security, Cyber Warfare and Digital Forensic(Cybersecurity)

AUTHORS PROFILE

Karthikeyan B completed his Ph.D in Computer Science & Engineering from SASTRA Deemed to be University, Thanjavur in 2015. He has published more than 40research papers in SCOPUS indexed journals and conferences. His area of interest is Image Compression, Steganography and Machine learning.

GOWTHAM G V is studying B. Tech Information Technology in SASTRA Deemed to be University, Thanjavur. He is very interested to study about Data hiding and Data Security in the field of Steganography. His area of interest is Steganography, Cryptography, and Artificial Intelligence.

Phani Teja R is studying B.Tech Information Technology in SASTRA Deemed to be University, Thanjavur. He is curious about Data Security and Data Protection. His area of interest is Steganography, Cryptography and Databases and data mining.