International Journal of Advanced Development in Science and Technology
IJADST Volume : 3 Issue : 03 April 2021 www.ijadst.com e-ISSN: 2582-1059

AUDIO ENCRYPTED IMAGE BASED ON STEGANOGRAPHY

[1] Rosini .S.K, [2] Yogeshwari.B, [3] Kapilavani.R.K, [4] Reena.R, [5] Dr. Ayyappan
[1,2,] UG Students, [3,4,5] Faculty,
Prince ShriVenkateshwaraPadmavathy Engineering College, Chennai, India,
yogeshwaribalaraman@gmail.com.

ABSTRACT

The protection of the message content is done by data hiding algorithm. To decrease the time of transmission, data compression is important. For few years, a replacement problem is trying to mix a compression, encryption, and data hiding in a very single step. So far, few solutions are proposed to mix image encryption and compression as an example. Nowadays, a replacement challenge consists to encrypt data in images. Since the entropy of encrypted images is maximal, the embedding step, considered like noise, isn't possible by using standard data hiding algorithms. A new idea is to use reversible data hiding algorithms on audio encryption into a picture. Recent reversible data hiding methods are proposed with high capacity and it is supported by steganography. In this paper, we propose an efficient data hiding technique and encryption within which the image and also the audio may be retrieved independently.

We have been used adaptive image filteringand adaptive image segmentation. this idea is predicated on both visual and statistical methods. High security layers are proposed through three layers to create it difficult tointerrupt through the encryption of the computer file and confuse steganalysis too.

Index terms: Reversible data hiding, security layers, audio encryption.

1. INTRODUCTION

Steganography is an art and science of knowledge hiding and invisible communication. It's unlike cryptography, where the goal is to secure communications from an eavesdropper by making the information not understood, steganography techniques strive to cover the very presence of the message itself from an observer so there's no knowledge of the existence of the message in the first place. In some situations, sending encrypted information will arouse suspicion while invisible information won't do so. Both sciences are combined to provide better protection of the knowledge. during this case, when the steganography fails and also the message can not be detected if a cryptography technique is employed.

To cover a message inside a picture without changing its visible properties, the quilt

source may be altered in noisy areas with many color variations, so less attention is going to be drawn to the modification. the foremost common methods to form these alterations involve the usage of the least-significant (LSB). the subsequent interesting application of steganography, during which the content is encrypted with one key and maybe decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key corresponds to the quantity of knowledge.

Therefore the main objective of the current work is the way to insert quite one bit at each byte in one pixel of the cover image and provides us results just like the LSB (message to be imperceptible). This objective is satisfied by building a new steganography algorithm to cover a great amount of any sort of information through JPG image by using a maximum number of bits per byte at each pixel. The information may be delivered over computer networks with little to no errors and infrequently without interference. Unfortunately, digital media distribution raises a priority for digital content owners.

Digital data may be copied with no loss in quality and content. This poses a giant problem for the protection of property rights of copyright owners. Watermarking may be a solution to the matter. It may be defined as embedding digital data, like information about the owner, recipient, and access level, without being detectable within the host multimedia data.

2. RELATED WORKS

In this [1] paper deals with the multiple data-hiders for RDH-EI based on secret sharing. It divides the original image into multiple different encrypted images with the same size of the original image and distributes them to multiple different data-hiders for data hiding. Each data-hider can independently embed data into the encrypted image to obtain the corresponding marked encrypted image. The original image can be losslessly recovered by collecting sufficient marked encrypted images from undamaged data-hiders when individual data-hiders are subjected to potential damage.

In this [2] This paper describes a novel high-capacity steganography algorithm for embedding data in the inactive frames of low bit rate audio streams encoded by G.723.1 source codec, which is used extensively in Voice over Internet Protocol (VoIP). This study reveals that, contrary to existing thought, the inactive frames of VoIP streams are more suitable for data embedding than the active frames of the streams; that is, steganography in the inactive audio frames attains a larger data embedding capacity than that in the active audio frames under the same imperceptibility.

In this [3] Low bit-rate speech codecs have been widely used in audio communications like VoIP and mobile communications, so that steganography in low bit-rate audio streams would have broad applications in practice. In this paper, the authors propose a new algorithm for steganography in low bit-rate VoIP audio streams by integrating information hiding into the process of speech encoding.

In this [4] Paper presents an improved multiplicative spread spectrum (IMSS) embedding scheme for data hiding. We first analyze the error probability of the conventional multiplicative spread spectrum (MSS) scheme and drive the corresponding channel capacity and security level.

3. PROBLEM DESCRIPTION

It is sometimes not enough to keep the message content secret. It is also necessary to keep the existing message to be secret. It is difficult to combine compression, and implementation of data hiding mechanism in single step. Hence we proposed a novel for hiding audio information into an image by the implementation of RDH methodology.

4. PROPOSED MECHANISM

Hiding the information within an image is most common procedure used at present. Through the internet secret messages can be spread easily by inserting the secret message in an image.To conceal a message inside an image without altering its visible properties, “noisy” areas which have color changes can be changed for the cover image the general technique used to make the changes engaged is the usage of the Least-Significant Bit (LSB), masking, filtering and transformations on the cover image The main aim of the project is to insert more than one bit at each byte in one pixel of the cover-image and obtain the results like the LSB. This aim can be reached by developing a Steganography algorithm to hide large amount of any type of information through JPG image by using maximum number of bits per byte at each pixel. Any type of data can be hidden in a JPG image which has 24- bits by using the Steganography algorithm. The 24 bits has three bytes of RGB colors, each byte has four bits called as Nibbles.

5. ENCRYPTION PROCESS

5.1. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) is implemented using MATLAB. encoding Standard (DES) is employed to implement cryptographic techniques since while, AES is that the advanced technology development for DES which is predicated on block cipher.

ALGORITHM

1. [s_ box ,inv _s_ box , w , poly_ mat , inv _poly_ mat] = aes _ init
2. Plaintext_ hex={‘00' ‘11' ‘22' ‘33' ‘44' ‘55' ‘66' ‘77' ‘88' ‘99' ‘aa' ‘bb' ‘cc' ‘dd' ‘ee' ‘ff' };
3. Plaintext=hex2dec(plaintext_ hex);
4. Cipher text=cipher(plaintext, w, s_ box, poly _mat);
5. Re_ plaintext=inv_ cipher(cipher, w, inv _s_ box, inv _poly_ mat);

5.2. AES INITIALIZATION

Before performing any original encryption or decryption the initialization function is called first.

The AES initialization [3], produces the substitution tables and generates the s- box which provides information of the constant vector and exemplary key. In this step two polynomial matrices are produced [3].

ALGORITHM

1.Function[s_box ,inv_s_box ,w, poly_mat , inv_poly_mat] = aes_init
2. [s_box ,inv_s_box] = s_box_gen;
3. rcon = rcon_gen;
4. key_hex = {‘00' ‘01' ‘02' ‘03' ‘04' ‘05' ‘06' ‘07' ‘08' ‘09' ‘0a' ‘0b' ‘0c' ‘0e' ‘0f' };
5. key = hex2dec(key_hex);
w= key_expansion(key , s_box, rcon);
6.[poly_mat,inv_poly_mat]=poly_mat_gen;

5.3. S BOX GENERATION

The substitution of bytes one by one of the similar finite field is done by the substitution tables. They use the expanded key functions for the encryption and decryption for the replacement.

ALGORITHM

1. function [s_box, inv_s_box]=s_box_gen
2. mod_pol=bin2dec(‘100011011');
3. inverse(1)=0;
4. for I = 1:255
5. inverse(i+1)=find_inverse(I,mod_pol);
6. end
7. for i=1:256
8. s_box(i)=aff_trans(inverse(i));
9. end
10. Inv_s_box=s_box_inversion (s_box);

5.4. FIND INVERSE

ALGORITHM

1. Function v_inv = find_inverse (b_in, mod_pol)
2. for 1 = 1:255
3. prod= poly_mult(b_in , I , mod_pol);
4. if prod = =1
5. b_inv=I;
6. break
7. end
8. end

6. MATHEMATICAL REPRESENTATION OF DATA

ARTHMETICS OF FINITE FIELD: A byte can be represented in different forms. A finite field has basic arithmetic's which are illustrated below. A finite field can also be named as Galois Field, which consist finitely many elements .The finite field GF(24) consists of the 24=16 with different numbers ranging from (0…16) which represents 4 bits. Special XOR and modulo-operations are used to check whether the sum and product of two finite field elements are in the similar range of the same finite field.hex2dec is a buit in function used in Matlab [3, 10].

7. IMPLEMENTATIOOFPRESENT ALGORITHM :

Assume that we have a cover-image which contains three types of MC: MC1, MC2 and MC6 and we have three types of pixels: MC1 with SC3, MC2 with SC5 and MC6 with SC1. Now, we try to hide 2- bytes 01010101, 01010101. Before weperform hiding, we must compute the number of segments in the Cover-image through the followingsteps:

Let L be a number of characters in the input password (PS).

Find N=round(L/2)

Find a number of segments on the vertical and horizontal directions (Segv , Segh) by using the following.

where, Val(PSi) represents the value of the ith character at the PS.

Find the size of non-uniform segments on both directions.

Perform segmentation by using column wise indexing on the cover-image into (Segv xSegh) segments through non-uniform size of segments. The present algorithm performs hiding into each segment separately according to row wise scanning.

8. SECURITY REQUIREMENTS

Encryption mechanism

- Adaptive segmentation of the cover-image
- Pixel selection style

Encryption mechanism:

The process of encryption is the first layer for security. Advanced Encryption standard algorithm provides high encryption to the data that is to be encrypted .

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

International Journal of Advanced Development in Science and Technology
IJADST Volume : 3 Issue : 03 April 2021 www.ijadst.com e-ISSN: 2582-1059

Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column

Adaptive segmentation of the cover-image

The second layer of security is the adaptive segmentation. The image taken as the cover image is the bitmap image and that cover image is segmented randomly of regular or irregular segments based on the password given or any other identification given by the owner. Irregular segmentation gives more security for giving the input

Fig 1: Segmentation

Pixel Selection Style

The third layer of security is the pixel selection. The Cover-image pixels are selected randomly to place the proper byte at its corresponding pixel to embed the secret data based on the colorcharacteristics of the cover-image.

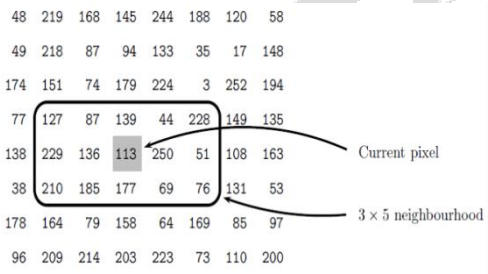


Fig 2: Pixel selection

OVERALL SYSTEM DESIGN

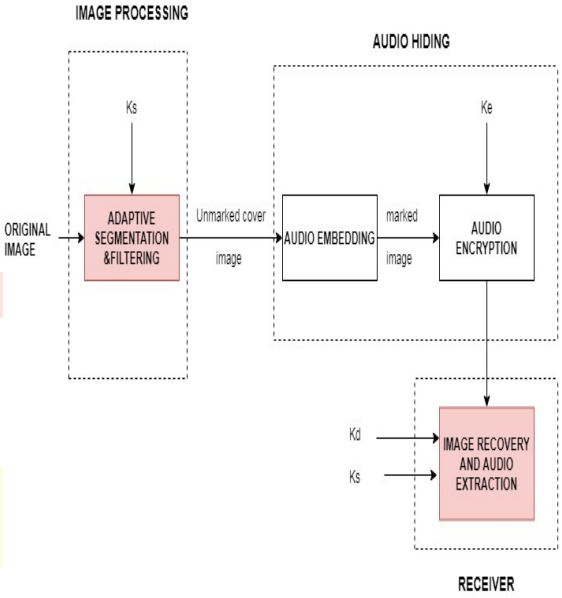
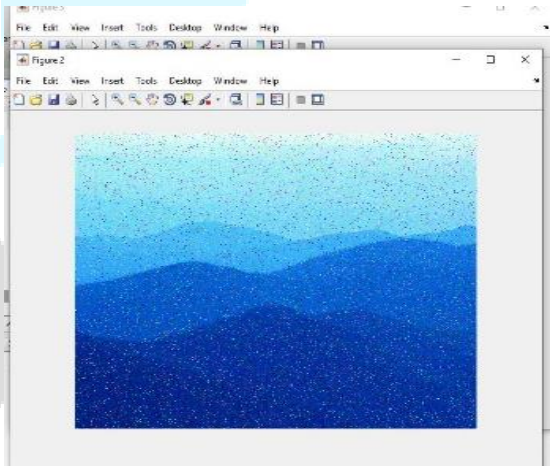


Fig 3: Architecture

9. IMPLEMENTAION AND RESULT

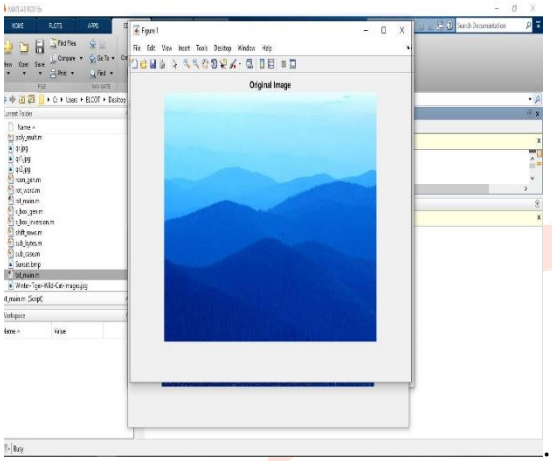
In this novel first Transmitter hiding the audio in to an image in an confidential information.

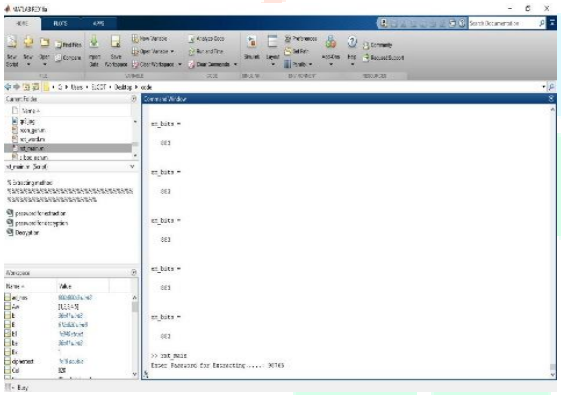


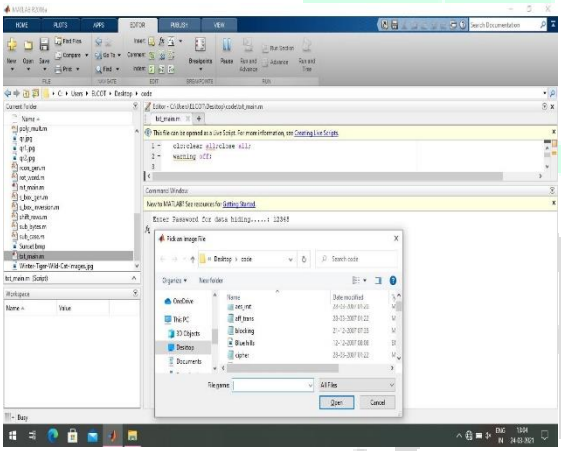
In this above Figure 4 the Receiver end needs an key to get an audio with an image.

The data received by receiver needs to insert decryption key to get audio and mean while also needs to insert password to view the

original image with lossless compression. The final output will be in two forms.







This Figure 5 represents the cover image with audio. In this Figure 7 image with audio can be the extracted by Receiver with decryption key. If the key not match with encryption key then it shows an error.

10. CONCLUSION AND FUTURE EXTRACTION

The proposed method modifies the amplitude of the cover image file to embed the secret message. To increase the security of the proposed scheme, we use a key to adjust the hiding technique. The experiment shows that our method is secure, imperceptible and can be used for hiding data in the image file. In the future research, we plan to use the error correction code to increase the robustness of this scheme. At the end, feasibility of image Steganography was evaluated by considering it's the pros and cons. In summary, if implemented correctly and in conjunction with cryptographic methods to secure the embedded data before insertion to a cover medium, many of the data hiding methods described above could become powerful tools for the transmission of undetectable and secure communication.

REFERENCES

[1] Y.-C. Chen, T.-H. Hung, S.-H. Hsieh, and C.-W. Shiu,"A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms," IEEE Transactionson Information Forensics and Security, vol. 14, no. 12, pp.3332–3343, Dec. 2019.

[2] S. Zheng, Y. Wang, and D. Hu, "Lossless data hiding based on homomorphic

cryptosystem," IEEE Transactions on Dependable andSecure Computing, 2019.

[3] K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images",Technical
Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004.

[4] An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[5] Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Jo rnal, February 1998.

[6] "Detecting LSB Steganography in Color and Gray-Scale Images" Jessica Fridrich, Miroslav Goljan, and Rui Du State University of New York, Binghamton.