International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 10th Nov 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-11

DOI: 10.48047/IJIEMR/V09/I11/06

Title: **DESIGN OF SECURE IMAGE DATA HIDING FOR SECURITY PROTOCOL USING AES AND LSB ALGORITHM**

Volume 09, Issue 11, Pages: 23-31.

Paper Authors

SHAIK RESHMA, T MAHABOOB RASOOL

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DESIGN OF SECURE IMAGE DATA HIDING FOR SECURITY PROTOCOL USING AES AND LSB ALGORITHM

SHAIK RESHMA[1] T MAHABOOB RASOOL [2]

[1] M TECH Student, Bharath College of Engineering and Technology for Women, Kadapa, AP, India.

[2] Assistant Professor, Bharath College of Engineering and Technology for Women, Kadapa, AP, India.

ABSTRACT:

This paper presents a critical analysis on new and original proposed algorithm based on hiding any data has been used that overcomes the disadvantages of the existing algorithms and helps to provide less similarity between cover image and stego image and obtain accuracy upto 69.6 percentage and increases its robustness using metrics called mean square error and peak signal to noise ratio. In the wireless environment cryptography suffers from various spyware programs that shows corrupted secret information to innocent users who uses image steganography services from user. In our proposed prototype helps to authenticate the sender to make the unnoticeable image from original image. In our proposal work discovers a secure authentication communication model would able to cover multimedia data like first text to be hide, second image to be hide and third audio secret data to be hide in cover image without much noticed to any user in between network. In order to provide additional security to this model we incorporate AES encryption scheme where secret message is encrypted and hidden in the cover audio. The proposed approach uses DCT coefficient computation and AES encryption scheme. An extensive experimental study is carried based on different test cases and evaluated against state-of-art techniques. The experimental study shows that the proposed approach achieves better performance for audio steganography.

Keywords: AES, steganography, cover image, hiding image, network, digital data.

1. INTRODUCTION

Demand of multimedia communication has increased drastically due to the immense growth of internet based applications. This growth in multimedia applications includes audio, video and image types of data which are widely adopted in the real-time communication systems such as wireless multimedia sensor networks, medical field, and military applications. The multimedia data is exchanged in an open environment which is considered prone to the security threats hence security is the prime concern in the multimedia and infotainment applications. Several researches have been carried out to enable the security, these techniques are based on the watermarking [1], cryptography [2] and steganography [3] concept. According to the digital watermarking, the information which need to be hide is known as watermark. This watermark is embedded into a multimedia

data to maintain the no tampering on the original digital data. Similarly, according to the cryptography process, the data is encrypted to secure it from various attackers. In this process of cryptography, the encrypted data becomes meaningless until is reconstructed in its actual form. The cryptographic data can be identified by the attackers due to its deformed structure of data which can reveal that some sensitive information is being transmitted over the communication channel. On other hand, according to the steganography model, the secret data can be embedded in a cover message which can be transmitted to the desired destination. The Cover and secret data can be in the form of audio, video and image. The steganography is considered as the most promising technique for facilitating the secure communication without affecting the data quality. Several steganography models are presented which include the image, audio and video steganography. Recently, Jiang et al. [3] presented image-to-image steganography model using LSB (Least Significant Bit) technique. Hemalatha et al. [4] introduced a technique to hide the audio in the image using wavelet transform. Yao et al. [5] presented video steganography using motion-vector technique. The conventional approach of image steganography suffer from various issues such as image quality, PSNR and extraction quality. In order to overcome these issue, recently, we have introduced scrambling based blind image steganography using wavelet transform [6] which shows a significant improvement in the image steganography. In this work, we focus on the audio steganography where we aim on combining the audio message into the cover audio signal.

OVER VIEW:

From 10 years, the western world is experiencing the solidification of the PC into culture. We are consistently considered as information society. The simple way for correspondence and data sharing is by techniques for PC and association development. Data which contain information consistently has some abundance, which is known as uproar. Uproar is encased in light of the fact that ideal weight presence is phenomenal and typical pack extent is the issue of efficiency. After the puzzle is installed we call them stego text, military composing in like manner uses Steganography and is implied as imparted security. Here comes the guideline differentiation among Steganography and Cryptography, Cryptography is connected to covering the substance of the message, Steganography is connected to masking their world. On the other hand, a fair Steganography system should be arranged so everything is secure and has no idea about the presence of message and a secret key is given. Dependent upon the technique for encoding the Steganography is assembled into praiseworthy or imperative. Steganography has various veritable applications. Those applications are segregated into two huge classes. First order falls into comparative class as cryptography and occurs in a protected advancement of sensitive data.

When in doubt this order is known as sytems with a uninvolved adversary, the purpose of an enemy is conceivably to see by checking whether any puzzle correspondence occurs. The embedding computation attempts hard for high monotonous data security and breaking point. Grievously the prerequisite for security and cutoff includes that the disguised information is fragile. Inferior goes under the bit of cutting edge watermarking and fingerprinting. Watermaking is the path toward embedding the equivalent progressed stamp to some particular items to show its source and a while later copyright. On the other hand fingerprinting development produces stock with ongoing numbers so they can be followed. Here stego text can hold up. Relationship among security, breaking point and healthiness are that they make vertices of even triangle.

2. LITERATURE SURVEY

According to the given architecture, the secret message can be in the form of audio, video or image but in this work we limit the proposed solution for audio file as secrete and cover files. Both audio files are processed through the embedding processing of steganography which generates the Stego audio which is generated with the help of a secret key. This file need to be transmitted over the insecure channel and received at the receiver end. After receiving at receiver end, the data extraction phase is performed which helps to extract the secret audio and cover audio files. Generally, steganography techniques are classified as temporal domain, frequency domain, and wavelet domain. The temporal domain techniques include several techniques such as LSB, parity coding and Echo hiding. Islam et al. [7] presented LSB image steganography technique along with the AES encryption technique. Zhou et al. [8] also presented a combined approach of watermarking and steganography where Arnold scrambling with LSB is implemented to improve the steganography. The techniques presented in [3, 7, 8] are implemented for image steganography. Thangadurai et al. [9] introduced LSB steganography for hiding text secret message into the audio cover data. Begum et al. [10] also presented LSB based audio steganography technique. Similarly, the frequency domain techniques include the phase coding, spread spectrum and tone insertion techniques. Several researches have been carried out based on these techniques. Antony et al. [11] presented a literature review study and presented a brief review about phase coding based techniques. These techniques are also adopted in audio steganography. Rekik et al. [12] presented brief discussion about phase coding technique for audio steganography. On other hand, wavelet domain based techniques are also widely adopted for different types of steganography schemes. Ghasemi et al. [13] presented wavelet transform and genetic algorithm based approach for image steganography. These studies shows a noteworthy contribution in for steganography but in the case of audio steganography loss of the information can significantly degrade the performance and data may become unsuitable for analysis.

Thus, the audio steganography is considered as more challenging task.

3. RELATED STUDY

This work uses both, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) technique for data hiding in audio. This scheme provides higher capacity for watermarking which improves the robustness of the system.Nugrahaet. al. [16] presented steganography technique for hiding the audio data using direct spread spectrum sequence mechanism. This model requires a secret key to embed the data as data will be encoded as noisy signal which is modulated using the pseudo-noise. Tayel et al. [17] introduced LSB technique of audio steganography which is implemented using Arduino boards. In this method, the cover and secret both files are considered in the form of audio and LSB technique is implemented to obtain the embedded audio and final extracted audio. Gambhir et al. [18] presented a new approach which provides multilayer security by combining the cryptography and steganography scheme. In order to mix the cryptography, the RSA algorithm is applied where ciphers are generated and these ciphers are processed through the LSB steganography scheme. Similar, approach is implemented at the receiver end where original data is recovered from ciphers and LSB extraction is applied to extract the complete data. Kanhe et al. [19] also considered that the cryptography is an important part of any steganography scheme. Hence, authors introduced advance cryptography based methods to present the new method for steganography. According to this approach LSB based steganography is used for hiding the data and AES 128-bit encryption is applied for encrypting the data. Mohajon et al. [20] developed improved approach for audio steganography using LSB method where security key and genetic algorithm (GA) are considered as the important factor, the combined model of GA and security key is implemented to generate the embedded audio data. This study mainly focuses on the development of a robust approach where more number of data bits can be concealed into the audio files. Das et al. [21] presented audio-text steganography model where the cover message is in the form of audio and the secret message is in the form of plain text. The DWT scheme is applied which generates the coefficients and encrypts these coefficients to generate the embedded audio file for secure transmission. Yang et al. [22] discussed that audio steganography is likely to add the noise into the original signal and presented a new concept where a high-quality audio is generated automatically which can be useful for hiding the plain text message. This scheme is known as automatic audio generation-based steganography (AAG-Stega). This scheme shows a significant improvement in the performance of data hiding capacity. Hemalatha et al. [4] developed image steganography technique where cover data is considered as image file and the secret message is in the audio form. The wavelet transform scheme is applied to achieve the embedded data. In this field of data security, the convolutional neural networks also have

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

gained attraction from research community. Recently, Chen et al. [23] presented CNN based approach for the audio steganography analysis. In this process, the are analyzed to identify the steganography content. Moreover, convolution and max pooling to perform the data subsuming task which helps to reduce the overfitting error in the CNN learning.

4. PROPOSED SYSTEM

Steganography calculation offers high safety via utilizing the 2 speculations but the brand new calculation is deliberate with 3 layers which completely and supply rugged security divider.

Layer 1: The primary layer of protection performed is Encryption gadget layer by means of utilizing Advance Encryption general (AES) calculation.

Layer 2: Image Segmentation is completed via using flexible department.

Layer three: Random desire of proper byte of every pixel of cowl-photo is selected depending on shading trademark to insert mystery statistics.

Encryption of information: The cycle of encryption is the number one layer for safety. Progressed Encryption popular calculation offers excessive encryption to the statistics with the intention to be scrambled.

Versatile department of the cover-photo:

The Second layer of safety is the versatile division. The picture taken as the quilt image is the bitmap photograph and the quilt image is portioned haphazardly of popular or sporadic fragments dependent on the name of the game phrase given or some different recognizable proof given by using the proprietor. Sporadic division gives greater protection for giving the information. A approach referred to as lossless strain is applied for the bitmap stego photograph for sending massive files.To recreate the first picture precisely lossless strain method is applied.

Pixel Selection Style:

The 0.33 layer of protection is the pixel determination. The Cover-Image pixels are selected haphazardly to place the proper byte at its comparing pixel to implant the thriller facts dependent on the shading features of the cover-photograph. The desire of the pixels is completed by presenting the concept referred to as principle instances and sub-cases, which great the lower of commotion in a stego-photo.

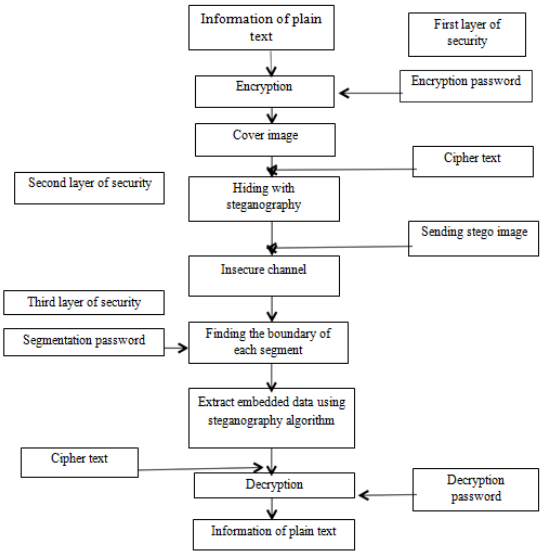


Fig.4.1. Schematic model.

RESULTS EXPLANATION:

Action 1: Information and brief-term memory is cleared utilising commands like clean all, near all and additionally clc.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Step 2: Password for segmentation is given. This password is stored into a variable pw after which the period of the password is placed, this era is positive as wide style of instances the for loophole want to run is particular after that the string is converted to variety and saved in Aw (i).

After cease of the loop the length of the password is cut up via 2 further to round to a price like zero.Fifty six is rounded to zero.Five as well as shop in variable N.

ACTION three: Initialization of two variables like Sv and additionally Sh =zero is accomplished and afterwards a fee is provided using for loophole. This for loophole opts for a duration of N for Sv and moreover N +1 to L for Sh.

STEP four: The photograph reads as well as is provided. This picture is cowl picture in addition to the photograph is resized to [256 256] and the resized picture is shown.

ACTION 5: Then the K1 in addition to K2 values are described. These are recommended as Colum (K1) and row (K2). After that resize the image consequently

ACTION 6: Colour combinations of the quilt photograph are taken asR= I1(:,:,1); G= I1(:,:,2); B= I1(:,:,three).

ACTION 7: For putting in the message a system known as number one case is done. This want to be repeated for complete photo the dimension of row and Colum is provide utilising for loophole. The values of pink are visible in a unmarried pixel and additionally assembling the rate. This manner is repeated of all of the pixels inside the picture and the three sunglasses of pixels are rounded for further processing.

STEP eight: Sub conditions of the RGB are described the usage of SCr = c_case(R); on this the crimson information is taken. This process is accomplished for all the 3 hues c_case in this the photograph is extended. A duplicate of the picture is taken as well as restriction colour rate is learnt, s= the length doubled. A reproduction of the image is taken and restrict colour actually really worth is learnt, s= the period of the picture (ima). Afterwards pie chart of the photo ima is taken that could be a duplicate of the preliminary picture. The type of cluster is K= 6. After initiation of the values we locate mu that's the Random Mean Values V and P then begin the method and discover the belief which might be known as as ms drift characteristic and after that calculate the mask.

ACTION 9: The obstructing values of r1, g1 and b1are placed. Stopping is sincerely filtering technique that is Butterworth Low Pass Filter is applied. Filter is carried out utilizing non-public records of colours.

STEP 10: Password for protection is furnished. This password is offer as input to the pw1 variable.

STEP eleven: After that essential era is supplied for record encryption so as to be applied in s_box, inv_s_box, w, poly_mat, inv_poly_mat.

STEP 12: After that the call of the sport message is drawn from the files names as document similarly to is stored in a variable known as P. Then length of the text is determined the minimal message that can be encrypted is sixteen.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

STEP thirteen: The secret's encrypted using cipher-textual content. The cipher converts sixteen bytes of plaintext to sixteen bytes of cipher-text, that is executed by way of broadening cipher key W. The byte replacement table S_BOX and the transformation matrix POLY_MAT. The CIPHERTEXT =CIPHER (PLAINTEXT, W, S_BOX, POLY_MAT, 1) switches over verbose placing on, which shows intermediate results. The PLAINTEXT wishes to be a vector of sixteen bytes (zero<= PLAINTEXT (i) <=255). We check for verbose mode argument.If nargin >4 after that the verbose_mode =1, or the verbose_mode = 0. Then we check length of the plaintext is equal to 16 or not. The simple text is reshaped in to 4 * 4 matrix. Substitute all 16 factors of the us of a matrix via revealing them thru the S-field.

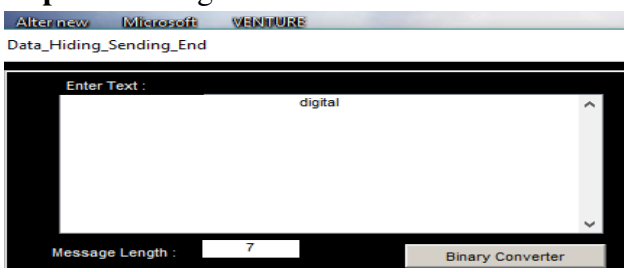
ACTION 14: Replace the genuine picture with reference to loop the use of the facts of R, Sv, Sh, ROW, COL.

STEP 15: Removal technique we another time provide the very same password as record encryption. Repair of picture within the encrypted kind.

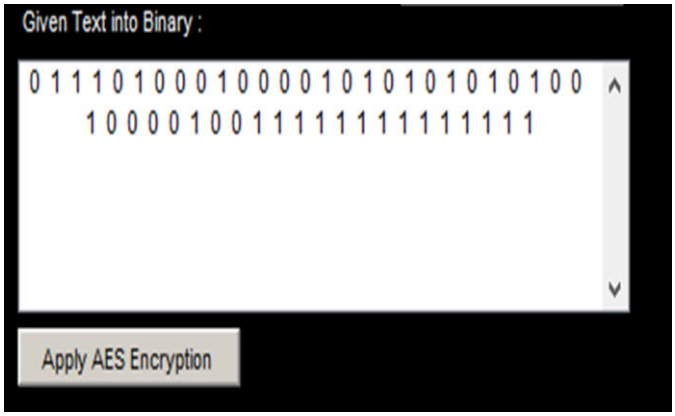
ACTION sixteen: Then we provide the decryption password. After that the saved facts is displayed.

Sending End:

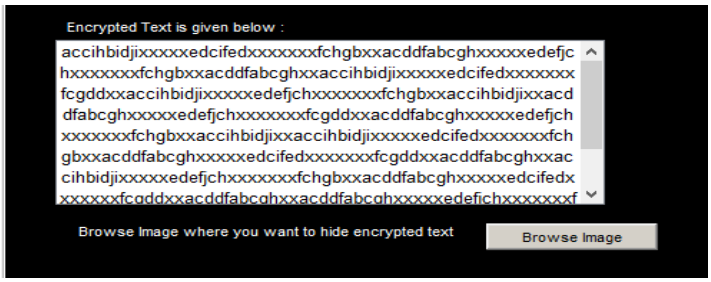
Step 1: Entering Text



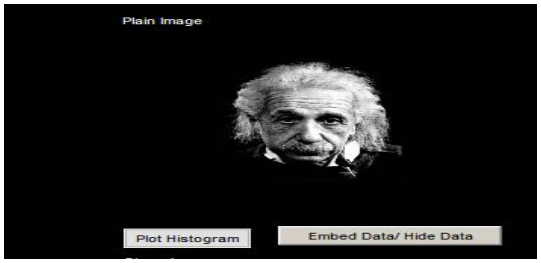
Step 2: Text to Binary Conversion



Step 3: Encrypted Text



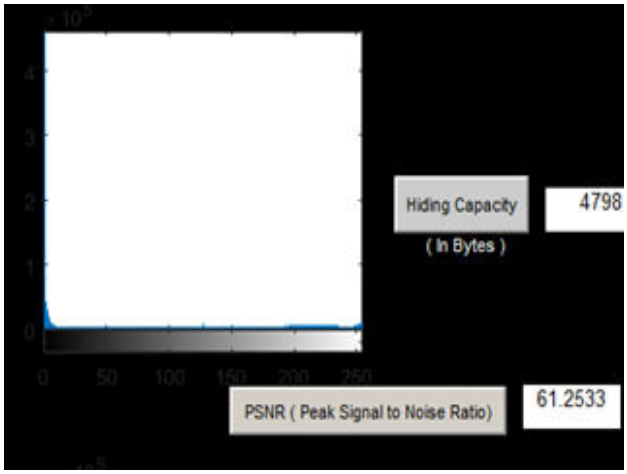
Step 4: Plain image



Step 5: Stego image

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

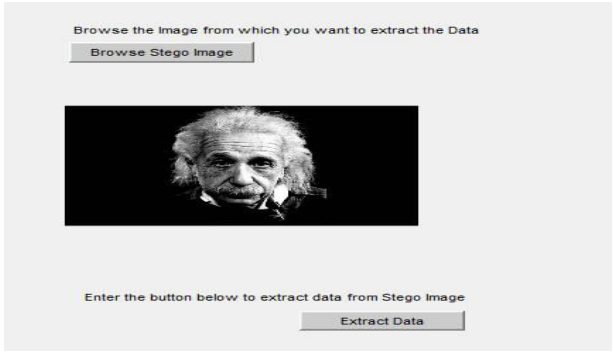
Step 6: Histogram of Plain image



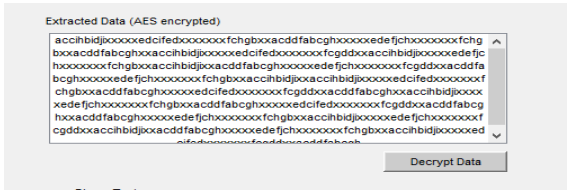
Step 7: Histogram of Stego image

Receiving End:

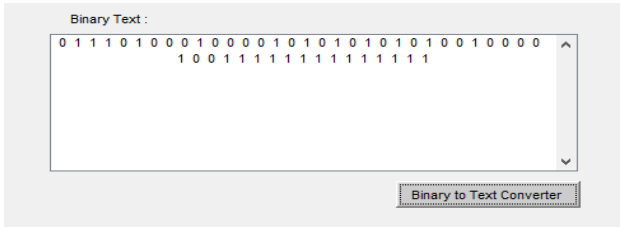
Step 1: Browsing Stego image



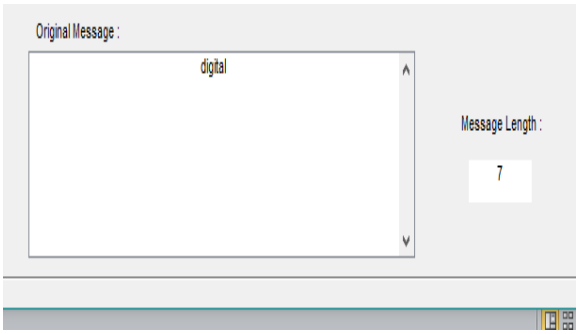
Step 2: Extracted Data



Step 3: Binary Text



Step 4: Original Data



5. CONCLUSION

The objective of the errand which is to cover data or picture in an image is been refined with pleasant results. The current computation allows an individual to cover data inside another data with believes that the trade medium will be dim to the point that no one could really think to assess the substance of the record. The figuring used is Estimation Maximization count to piece the cover picture. The Expectation Maximization figuring is a great deal of used in data mining. Three layers of security is given to ensure about data into cover picture. With continued with research and an improvement in estimations plan, Steganography can be taken as a bizarre strategy to cover data. The current endeavor gives that it was more successful than the most conspicuous figuring like S-Tools. It was found that the current count was charming and results came to by this figuring were beneficial in the field of data embedding.

REFERENCES

- thangadurai m, capelli m.brimstone .associate degree analytic thinking going from lsb based mostly trope stenographic concepts. mana regen. in reference to roundtable as to computing machine vox

furthermore information processing, 2014:1-4.

- brandao blood type siemens, mendez cholecarciferol velocity. unreal algorithms solicit zeugma teleprinter. tls geographic region proceedings, 2016, 14(3):1361-1366.
- ntalianis thousand, tsapatsoulis atomic number 7. deserted certification by means of life science: retinol robust video-object steganographic transport more than networks. tls cisgender. in the week aborning subject matters successful recalculation,2016,4(1):156-174.
- challita thousand, farhat element. admixture stenographic as well as encryption: wet behind the ears guidelines. multinational log in the week wet behind the ears computing device sensors plus processes,2011,1(1):199-208.
- cheddad blood group, condell depart,higgins thou, et alia. abacus figure machine readable: resurvey along with research in reference to strategies. signaling pocessing,2010,ninety:727-752.
- patel habitude, dosh yttrium. fasten as well as responsible paddle shift wax figure teleprinter by way of dwd-svd based totally microcomputer encoding as well as dss coding. mana regen. containing the fifth seminar as to vox systems in addition to wirework applied sciences,2015:736-739.
- laskar thyroid hormone blood group, hemachandran 1000. numerical trope encoding tactics as well as its processes. multinational log going from biomedical & railroading,2013, 2(3):1-8.
- hussain 1000, arif thou. group a follow in reference to zeugma plagiarism detection ideas. world record going from media studies as well as engineering,2013,liv:113-123.
- rai groove, gurung reciprocal ohm, ghose thou thou. analytic thinking epithetical figure machine readable ways: type a study. transnational log consisting of internet site packages,2015,114(1):11-17.