A Secure Framework for Communicating Multimedia Data in Cover Images using Hybrid Steganography Algorithms in Wireless Local Area Network

Jagadish Gurrala, Pasala Sanyasi Naidu

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. The proposed algorithm has been tested against various existing algorithms to develop how effectively the hybrid steganography algorithm is works, and how effectively it is overcoming the drawbacks of the present image steganography algorithms. The present work is projected to serve the purpose of prevention of changing secret data in cover image after evaluating the distraction values using PSNR and RMSE quality metrics under various image data set taken from facebook shared images . In the scientific investigation, researchers found that three reasons to show that given secure communication is successfully designed with the help of hybrid steganography algorithm that could break attackers intention using TLNUS merged with AES and Key based positioning system[4] gain access the sensitive information available in remote system

Keywords* : *Image steganography, TLNUS, KPS, Wireless LAN Wide Area Network.

I. INTRODUCTION

the wide propaganda of Information Critical and Technology (ICT) in 2019, all over the continents, Network security became one of main issue to be considered. In Wireless environment Multimedia information Hiding in Cover images addresses many research gaps provided third party may intercept images through using image manipulations tools. Still images i.e cover images provide a relatively small host signal(Cover Image) in which to hide multimedia data only text or image. For example an 256-bit cover image supports[3][11][12] upto 996 X 667 pixels provides approximately 6 Mega bytes of multimedia space in which to communicated using traditional steganography. Each pixel in the image is represented as a 24 bit map value, composed of 3 bytes representing the RGB values for 3 primary color channels Red, Green and Blue respectively. Now, the question arises that how to secure these pixels which displays in images of computers. When using cryptography deals, it is not safe towards handling malicious cipher content[10] introduced by hackers or intruders in any of the wireless system, that contains key logger programs, spyware programs like virus or worm could spread across computers connected in wide area network and it may cause damage of the specific computer leads to victim network and it will definitely leads to malfunctioning of the system. Within no time entire network goes out of control from the users and gets destroyed thus losing all confidential data Because of this the efficiency of the system goes down. So such is the importance of the establishing security policy for the systems which achieves the authenticity problems.

The main goal of this paper is that it should hide all multimedia data using hybrid steganography working in wireless environment like 802.11 standard, all they exist in the any system in the network(WLAN) and immediately stop them from spreading all through the network. In this paper, we suggested that the required inputs are existence of image manipulation tools and the desired outputs are avoid the difference between stego image[3][4] and cover image. If big enough secret multimedia data is able to hide and to be transferring over the wireless network, it will be create tamper proof image transfer even hiding any multimedia.The majority of data hiding techniques for the concealing of secret multimedia information would communicate to authors suffer from not upholding secret data to carry across WLAN. This study presents a hybrid steganography algorithms for high hiding capacity of text files, image files and audio files in cover image file (all together called multimedia files). The proposed methods are carried out using two methodologies[27-45]. Cover file (Color or gray scale image file of capacity starting from 20K to 2MB) is segmented into uniform blocks and these blocks are hidden after encoding with AES algorithm. The work is further extended by considering the encrypted text in non uniform segments using cipher keyCk.

Revised Manuscript Received on December 13, 2019.
***** Correspondence Author
Jagadish Gurrala*, Research Scholar, Dept. of CSE, GITAM Deemed to be University, Vishakhapatnam, India,.
Dr. Pasala Sanyasi Naidu, Dept. of CSE, GIT, GITAM Deemed to be University, Vishakhapatnam, India,.

Further research is carried out by considering the embedding multimedia file into a Cover image file. The results derived are competed and performances of the developed modules are evaluated.

II. BACKGROUND AND MOTIVATION

In the scientific investigation, researchers found that three reasons to show that given secure information communication is successfully designed shown in fig 1 with the help of that system could break that system using gain access the sensitive information available in remote system. In essence some problems were raised due to spywares were identified by malicious intent held in some computers. Therefore these virus or worms could be identifying by using antivirus software and stringent rules obtained by firewall discussed in techniques of steganography [W Bender et al., 1996] are a solution for this problem.

- An undesirable effects on carrying copyrights materials across internet.
- Patent transfer across internet as well as storage.

Least Significant Bit Substitution Technique (LSB):

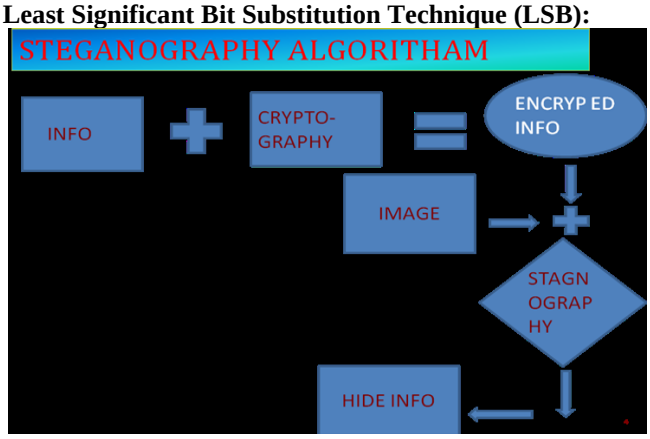

Figure 1: Steganography Operation with Cryptography Key

III. LITERATURE SURVEY

Information hiding is a class of process where multimedia data file is classified into outer file and inner file. Outer file is visible to external world and inner file is visible to content receiver for the sake of attaining authentication, confidentiality and improve the imperceptibility of inner contents. After reviewing many research studies and getting the knowledge about how to make the internal security to any kind of communication using various techniques for data hiding shown in fig 2, it is understood that it is necessary to put efficient feasibility using these strategies to attain good information hiding concept rather than data hiding concept. Less research happened to dig the information hiding knowledge for tamperproof security.

The research survey[4][7][14][16][18][20] shown that if the text is taken as a carrier, it couldn't carry enough inner content to get it travel across network because text has limited features in it. In audio carrier, huge research happened. In this context, it is found that audio shelters couldn't be carry enough details in cover media as sound wave is heard even though the audio spectrum details are modified. The video steganography also not a suitable technique to carry inner details over internet, since it suffers difficulties to put video frame in group of sequence of image frames in it. In this connection, the image is a convenient carrier to conveying details in secure communication. Modern image transfer techniques would be successful to carry information to convey details across network with less effort compare to any other multimedia carriers.

According scientific investigation on Data hiding techniques, researcher's addresses a need of huge research is required to challenge to hide large amount of inner data to be travelled across network. Nevertheless, regardless of its historical value and potential benefits, the steganography is rarely used and can hardly be assessed in the current era. In addition, it would be difficult to employ that older technology with modern computer, due to changes in operating systems and processors. These concerns about the distortion rate and usability of the data hiding techniques prototype denote that the application of a multimedia form of data hiding possesses a higher invisibility for the research purpose of the present study if a embedding capacity is increased in a host image still be of interest of future studies.

- Personal, Private Data to be kept safely:

Ex: Pokemon Go → real time game

LSB algorithm Complexity is depend on amount of key and text it is approximately equal to Big O(m*n) where m and n is size of cryptography key and given secret multimedia content respectively. After the converting our multimedia content in secret code or encrypted form researchers were needed to patch that multimedia data in the cover image. We use least significant bit for the patching of data because of following reason.

a. Because the intensity of image is only change by 1 or 0 after hiding the multimedia information.

b. Change in intensity is either 0 or 1 because the change at last bit .e.g.

11111100 → 11111001

Least significant bit (LSB) insertion is a old approach suffers from carrying enough data (i.e beyond 34 %) across internet. Until now many researchers work on bmp and GIF images as cover images to make it data remain hidden. But keep on increasing embedding data(payload) could decrease the image quality and robustness. Thus Existing approaches works quite well in Lossless images and may not work well in Lossy RGB images(JPEG) with related colors.

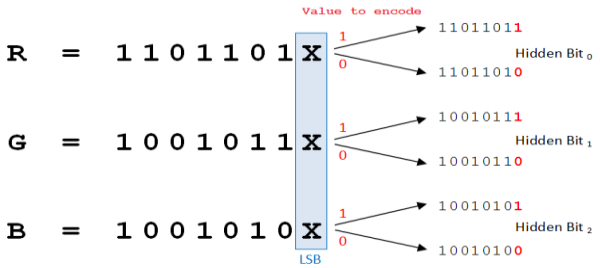

Figure 2: Least Significant Bit Substitution Process

The present research work is aimed at proposing methodologies (TLNUS) is based on little flavor of least significant bit substitution process shown in fig 3, for safe guarding information, such that no secret data is modified and thereby the security of the data can be further strengthened. This paper

work is further extended by inserting the audio in the image, and the results are derived and compared.
The take a break of the paper is structured as follow: segment 2 discusses the literature survey of Text, image and audio steganography from existing Image Steganography system and their limitations with respect to the security. Segment 3 describes about critical analysis and the proposed model are presented in Segment 4. Finally we conclude this paper in segment 5.

IV. EXISTING SYSTEM TO HIDE TEXT AND IMAGE IN MULTIMEDIA COVER DATA –CRITICAL ANALYSIS

Authors have been surveyed on several data formats(either text or image) hiding techniques, in the form of steganography. In the existing algorithms identified two problems, either some algorithms only deal on embedding text file in cover image or some algorithms deal on embedding image file in cover image. In the proposed methodology called Hybrid approach of TLNUS and AES, ability to embedding text file and image file inside cover image to got better results.
Each pixel in the image is represented as a 24 bit map value, composed of **3 bytes** representing the RGB values for 3 primary color channels Red, Green and Blue respectively.

2.1 TECHNIQUES ON MULTIMEDIA HIDING - LITERATURE SURVEY

1. In last 4 decades, scientist conceived idea of introducing 26 alphanumerical letters is fuel for communication during embedding user defined text.

2. In Multimedia Steganography[8], original content include text,image,audio would follow context free grammar notation to add up sensitive text in cover file shown in figure 3.

3. Unable to trace defined path: When authors inculcating text need to have user defined way to put up details. Therefore it is difficult way to finding text.

4. Scripts injection: Enclosed text delimited by Less than mathematical symbol and Greater than mathematical symbols to enable extra buffer to lock scripts for injection for text hiding.

2.2 Existing System to hide Audio in multimedia cover data – Critical Analysis:

Authors look on survey on several data (Audio) hiding techniques. In the existing literature study, most of the algorithms only dealt with embedding audio file in cover audio.

2.2 .1 Pitfalls in LSB methodology:

In this paper, there were identified 2 weaknesses in Least significant process:

1.Only read the 0^{th}position,1^{st} position and 2^{nd} position of all red , green, blue channels of 3D array to retrieve the portions linearly and then arrange these index position of three dimensional array and put it in serial order to get sensitive text details in cover file.

2.Using image processing code in Matlab, to have instruction called imread(x.jpeg), impixelposition() to read location information i.e coordinates of two dimensional pixel details of stego object , from that all least portions of string of arrays are poured into temporary buffer to another buffer for disable steganography [Neilson, 1998].

3. There are various information hiding approaches have been added to get security while using cryptography.

4. Least significant method[1] shows outstanding methodology upto 1990 year, after there are many researches survey discovered and survey a lot.

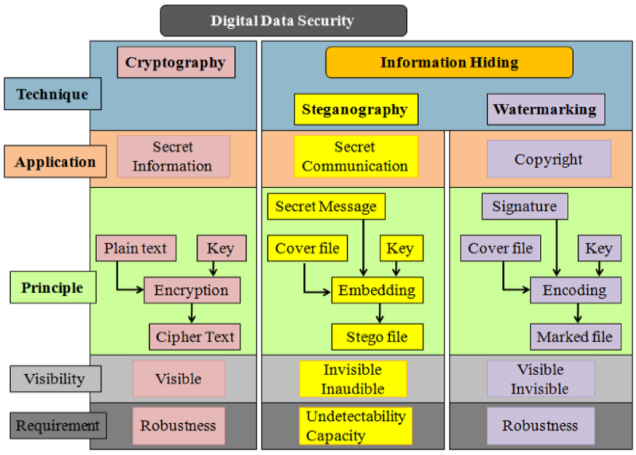

Figure 3: Illustration of Evolution of Digital Data Security Approaches

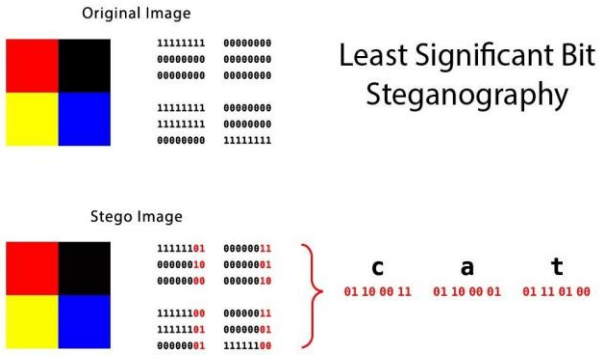

Figure 4: Apply LSB positioning Model on CAT text is hidden in Original Image

The letter 'c' has an hexadecimal code of 0x36,0x37 to be transform to binary called 011010011. In insertion process add the character 'c' into the cover RGB file mentioned in Fig.4.Why because each image pixel location can address two bits of least portions of cover file for storage as well as retrieval. Two pixels were enough to embed secret text details. Similarly letter a and letter t has a common operation to place it requires 12 pixels. In recent literature survey (champakamala 2007, Chatterjee, 2008) address the least significant coding wouldn't meet the requirements of lack of space to embed details. Researchers were survey existing techniques which doesn't support Red Green Blue color channels provide perfect hiding techniques in different versions of images such that Each color has individual intensity values such as: R = 97, G = 186, B = 318. In this regard

it is vague process in LSB substitution. It is fundamental fault rules out in LSB process. So that authors designed individually handle locations to place sensitive information in it. In the proposed methodology called Green color based key position algorithm, ability to embedding audio file inside cover image to got better results .

The incidence of cryptography attacks has increased in last two decades due to the more awareness has been penetrated to hackers[19] and their strategies. In this connection, hackers could deploy exploits in all platforms i.e web world, software application, human factor, hardware security system. So many problems occur [13][14] faced the challenges to the corporate companies.

V. COMPARATIVE ANALYSIS ON EXISTING METHODS

3.1 Various Data hiding approaches in Image steganography:

In the survey the various algorithm could not accommodate multimedia data simultaneously because of vague of ideas shown in table 1.

Table 1: Analysis of existing multimedia content hiding approaches

Cover type/Secret content type	Multimedia Data hiding approaches
Text as a cover / Multimedia content	Morse code (fallen grass, Standing grass notation), Alphabetic shifting, space conversion, In the survey various textures like wax covering, hair grow methods and patch work [14] methods only hides data upto 33 % to the existing cover image.
Image as a cover media / multimedia content	Image hiding techniques having little room to accommodate inner image information to hide in cover image.[2-9]. There are several methods to hide image inside cover image.
Audio as a cover media / multimedia content	Most of the algorithms were focused on Discrete Wavelet Transform techniques are used for hide audio within the given cover audio file[Hemalatha et al.,2015].[11-16]
Video as a cover media.	Research in progress[19][20].

3.2 Data Security gap analysis:

They [24-35] observed following excerpts during Data Security gap analysis:

1. For entire years, Human observer always sees the remote computers activity details in 24 * 7 manners shown in table 2.
2. Known bit positions of cover media suffers with lot of steg analytic attacks to make it possible to handle details using new tools derived from base tools.
3. To get the clarity on stego object pixel variations so that which key is turned the cover carrier into concealed form using huge study on integrated approaches of cryptography with steganography.
4. After finding results from investigation on still images, there is a lack of security mechanisms to hide inner information to uphold text/image/audio inside cover image file.
5. In the gap analysis, authors analyzed the space and time complexity for those techniques to stabilize the complexity into simple technique through understanding basics of methodologies.

Table 2: Security services aspects between Steganography and Cryptography

Hiding technique Type	Confidentiality	Integrity	Time Complexity	Space Complexity	Authentication
Steganography	May be	Obvious true	Medium	Medium	Obvious true
Cryptography	Yes	Yes	High	Less	Yes

3.3 Data Hiding Techniques on Multimedia hiding Processes:

Binary based steganography to hide multimedia data organized in such a way that all pixels of binary image[3]. The key metrics to measure the amount of data in evaluating to put multimedia data to be hide, the perceptibility of the given secret multimedia data, and its strength can maintained in the properties of communication systems: information carrying capacity. In the given paper context, the hidden multimedia authors are setup to trying to hide is the how much multimedia content ranging from 1K to 343 K bytes data have been chosen to carry the information carrying capacity over network and the cover image is viewed as blurred image. However, dissimilar thing is to distinctive communication test cases where a high PSNR is appropriate with slightly less PSNR for a image steganography corresponds to lower visibility and consequently better achievement when data hiding in the implanted multimedia data. The assess of payload capacity can be worn to illustrate a rank of toughness whether to eradicate the implanted secret multimedia, premeditated or inadvertent.

3.4 Constraints of Text and Audio Steganography:

According image steganography paradigm authors given various results taken from pixel adjacent algorithms[16] and particle swarm optimization algorithms[17] have been used to hidden multimedia data within the original image. The metrics like peak signal to noise ration and payload capacity of cover image audio signal is to hidden upto -49.6 decibels from -9 db onwards when we were using different sizes of multimedia contents within 2019 * 1987 image dimension. it supports bit error rate upto 0.25 and could accommodate 8 million samples in cover image.

VI. PROPOSED METHODOLOGY USING HYBRID STEGANOGRAPHY

The most effective method of hiding secret content is by kept it in Image as a container to transfer the secure data across

networks. In this way the characteristics will framed and could deploy these systems to eradicate the strategies of hackers world and to maintain persistence of data before and after adding it. Authors proposed two comprehensive algorithms i.e Two level N on Uniform Segmentation (TLNUS) and AES algorithms would keep text and image in Cover Image and another comprehensive algorithm is Key Positing RGB and Gray Scale Image steganography shown in figure 5 for hiding audio in Cover image.

This paper investigates the various ideas [2-8] of hiding techniques and then analyses the most common forms multimedia content as a secret information kept in cover image, such as watermark, fingerprint. To assess the robustness of cover image even after hiding multimedia data as secret data using metrics of image quality concept[12]. Until now sensitive data can't be send inside an Cover image through proper means that satisfies the secure measures such as authentication, confidentiality. Cover Image (Still image) is familiar aspect in Steganography where hidden details will be kept safely rather than cover audio file or cover video file. Authors proposed two secure frameworks in image steganography where a person can send text, image and audio file inside Cover Image with simple and efficient approaches. First framework designed three tier architecture to make hide secret data into cover image file and second frame work is to connect all three different files of content into secure places of image using cryptography methodology such as 128 bit advanced encryption standard.

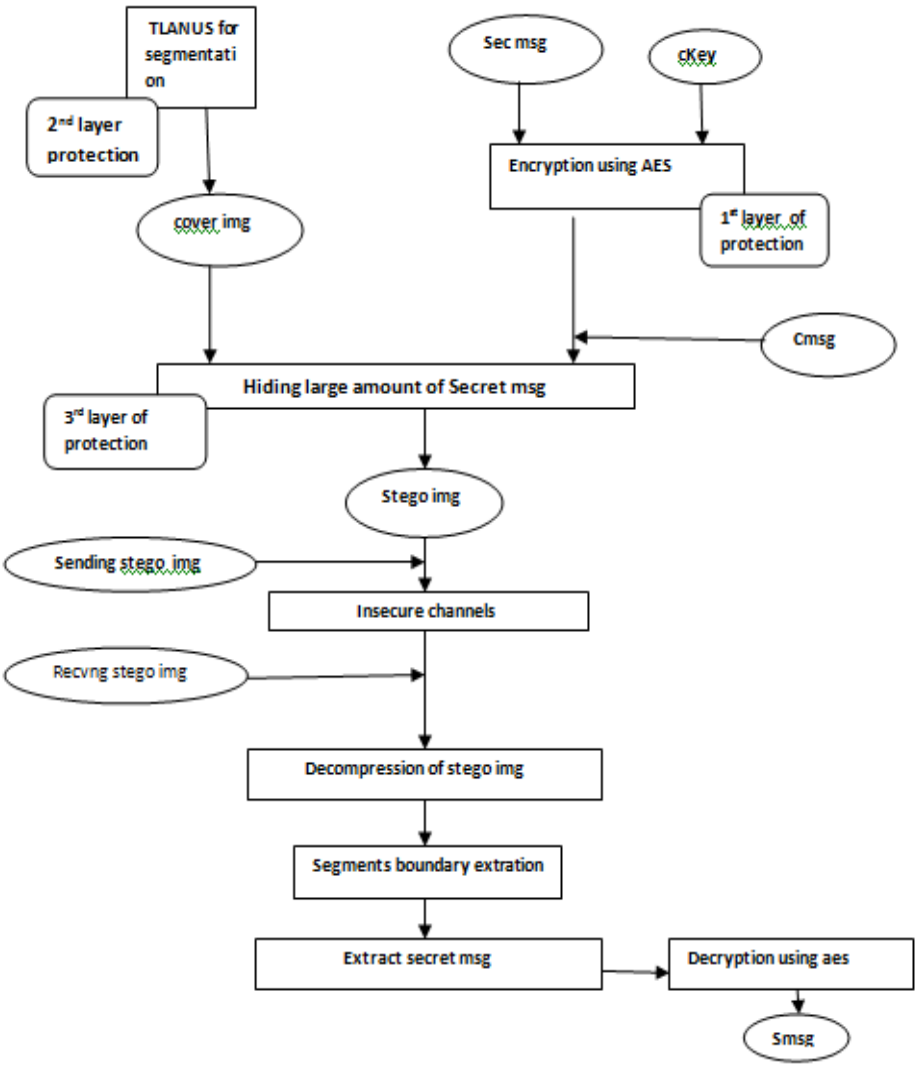

Figure 5: Secure multimedia hiding model

Hence authors decided to choose image as a cover data to hide any kind of multimedia information such as copyright [10-15] information image, audio, or text with a minimum amount of perceivable degradation to the Cover Image.

1. First framework is used to create positions of image where secure multimedia data can accommodate it in segment locations for Authentication.
2. Enciphering of data for more confidentiality using AES.
3. Embedding data requires- identifying segmented portions (edge) of image Using obtained values of Sizes of Horizontal Segment (SHS) value and Size of Vertical Segment (SVS).
4. Sending the stego-image.

4.1 Hybrid Steganography Evaluation Process:

4.1.1 Calculation of Segmentation size of Image parts:

From the table 3, the whole image is subdivided into n non uniform segements in terms of vertical segments and horizontal segments starting from 1024*946 resolution

contains less perception than other images shown in figure 6.

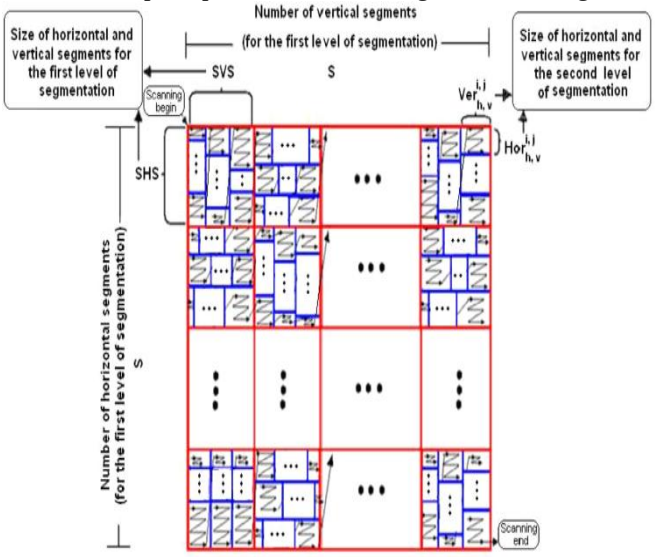

Figure 6: Calculation of proposed width and height of SHS and SVS through TLNUS formula.

4.1.2 Proposed Algorithm:

1. Data embedded preparation

1 For each horizontal element in Original image contains rows r=0,....Max and column c=0,….,Num

1.1 For each row r=1,….,Max

1.2 For each column c=1,....Num

1.3 For loop on decision value for segmentation k = 1 to L(odd prime number)

2. Vertical(Wi) size computation on original cover image:

2.1 (Wi(0),Wi(1),...,Wi(18)) = Message[k] /* Divide M[k] into 18 horizon segments */

2.2 For t = 16 to 79 do:

2.2.2 Wi(t) = (Wi(t-3) XOR Wi(t-5) XOR Wi(t-7) XOR Wi(t-16)) <<< 1

3. Horizontal size segment computation on original cover image:

3.1 AES = Horizontal segment0 (H0), similarly BIG (vertical segment) = H1, CIP (Key size) = H2, D (secret data size) = H3, E (pattern of embedding of image) = H4

3.2. For transition value = 0 to 79 do:

3.3 Stego Image locations = AES<<<8 + f(t;BIG,CIP,D) + E + W(t) + K(t) E = D, D = C,

3.4 CIP = BIG<<<30, BIG = AES, AES = stego image locations

End of for loop

1. Extraction of location when stego image is reached:

HIF0 = HIF0 + A, HIF1 = HIF1 + B, HIF2 = HIF2 + C, HIF3 = HIF3 + D, HIF4 = HIF4 + E

Terminate the control of the body

Output:

HIF0, HIF1, HIF2, HIF3, HIF4, HIF5: Word buffers with final stego image.

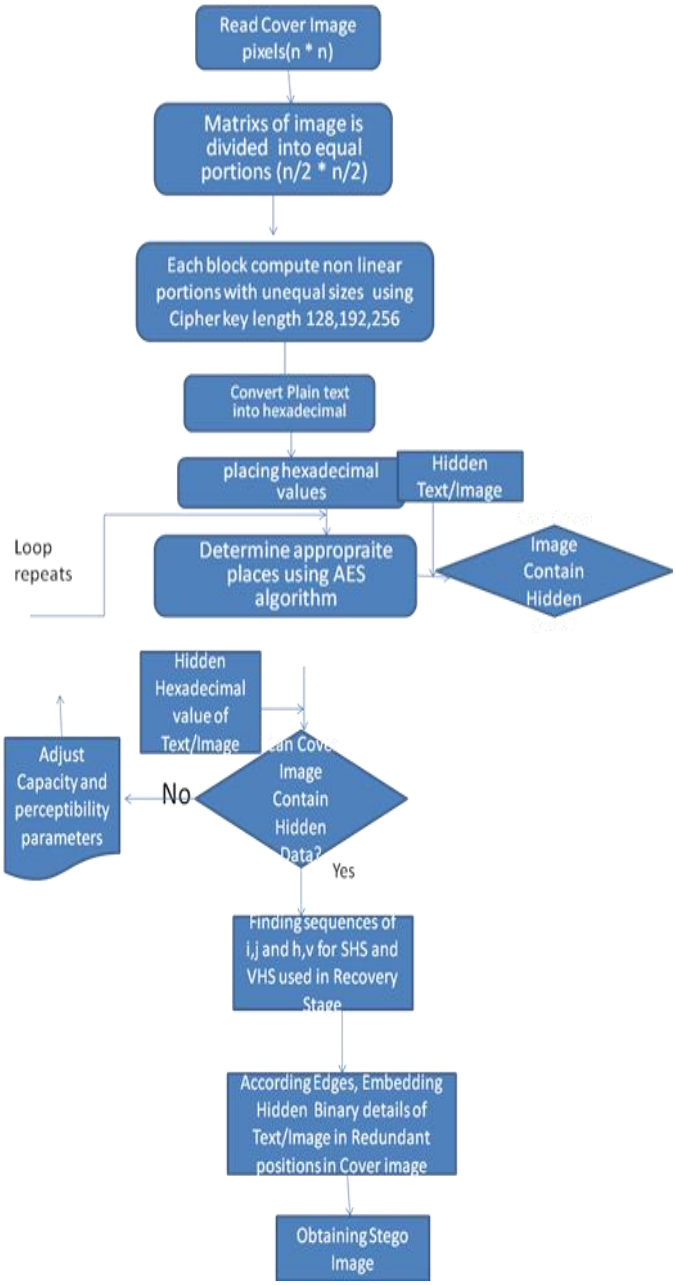

Figure 7: Flow chart for adding secret image into Cover image for secure framework

4.2 Comparative analysis on hidden images :-

Table 2: Comparative analysis of hiding multimedia data inside Still image

Algorithms Techniques	Cover Image	Stego Image	Secret Image	Available capacity	PSNR	RMSE
Li et al 2013–	Image5.jpg 512 * 512 (768KB)	Stegimg4.jpg 365KB	130KB (image)	Upto 25 %	38.987	22.89

Nameer L.Emam(2015)	Image5.jpg 512 * 512 (768KB)	Stegimg5.jpg 310 KB	130KB (image)	Upto 75 % space	42.473	6.893
J Gurrala et al., 2019	Image5.jpg 512 * 512 (768KB)	Stegimg6.jpg 278 KB	130KB (image)	Upto 83 % space	50.876	0.893

From the three latest papers survey reports according Li et al 2013 survey the various cover images of sizes Image5.jpg of size of 512 by 512 with 768 kilo bytes which carries upto 130 KB images having less peak signal to noise ratio 38.987 with high mean square error of 22.89. However according Nameer et al 2015 survey the various cover images of sizes Image5.jpg of size also supports 130KB inner image having medium peak signal to noise ration 42.473 with medium mean square error of 6.893. Finally according proposed method support same secret image produces better results in the sense the Peak signal to noise ration having more values i.e 50.876 ideal situation and 0.893 produce ideal situation it seems. Hence from the critical study our paper support the methodology [16] which convey upholding the content for safeguarding details.

4.3 Experimentation setup:

There are 4 modules were designed[5][8] and implemented[6] to hide multimedia into cover image as follows.

1. To provide required authentication using first secure architecture to create positions of borders of given cover image to place secure content.
2. To provide required confidentiality using Advanced Encryption Standard.
3. To achieve the zero differences between cover image and stego- image file through quality measures.
4. To prevent access to cover image through secret multimedia content by having cipher key locations generated by 128 bit AES encryption method.

VII. RESULTS

In the experimentation, it is taken 6 images with color information ranging from 64.4 K to 343 K bytes of cover images img1e,img2e,img3e,img4e,img5e,img6e which carries 50 different text,50 different images,50 different audio sizes of multimedia contents shown inf figure 8.

Figure 8: cover images for creating secure positions in cover image

Figure 9. stego images when deployed the content.

4.5 Determination of Metrics using Formulations:

- After expermentation the proposed hybrid steganography works, authors mentioned metrics like PSNR,RMSE.
- For , High value of PSNR (decibel) is having less value of RMSE.
- For Ideal situations, PSNR = as large as possible. MSE = 0 to +ve
- In the proposed methodology shows better results when creation of stego-images.

5.1 Peak signal to Noise Ratio:

Peak Signal to Noise Ratio $=10 \times \log_{10} \frac{MAX^2}{RMSE}$.

for all values of MAX starting from 0 to total number of pixels in cover image.

RMSE $= \frac{\sqrt{\sum_{i=1}^{n}(Pi-Oi)^2}}{n}$

for all values of P_i comprises distorted image pixels from 0 to

total values and O_i comprises original pixels starting from 0 to total values from 0 to total.

Table 3: Evaluation on image data set after adding multimedia secret data

Co ver (.jpg)	Appended data(txt/aud/jpg) size in K bytes	Approximate error values	Bit error rate	Root mean squre error
U1(962)	Ue(172)	1.2009	233	844.2
U2(897)	Ue1(197)	1.0999	231	977.7
U3	Ue2	1.088	228	990
U4	Ue3	1.0322	223	1.22
U5	Ue4	1.0011	221	1.20
U6	Ue5	0.2331	219	2.55
U7(3090)	Ue6	0.2009	212	3.66
U8	Ue7	0.0199	210	2.77
U9	Ue8	0.0162	206	2.55
U10	Ue9	0.0011	204	2.5998
U11	Ue10	0.0005	203	2.11
U12	Ue11	0.0003	201	2.09
U13	Ue12	0.0002	198	2.766
U14	Ue13	0.0001	296	2.456

From Table 3 the experimental results shows that authors tested 14 cover images i.e U1,U2,upto U14 images which holds Ue,Ue1,Ue3..Ue13 having less robustness through root mean square error value of 844 and increases the cover image size to decrease the root mean square error form 9.154 to 2.456 approximately. After adding different sizes of secret multimedia shown in Figure 10 after adding 56 bytes of data from 64.4 multimedia content the payload is suddenly increased from 39.7 % onwards.

Table 4. Payload capacity for different sizes of multimedia contents for cover images.

	RMSE 1(Existing audio Hiding Algorithms Lee and Tsai, ANN_MPSO)	RMSE 2(Proposed audio Hid Algorithm _TLNUS_AES)
10%	9.154	8.364
20%	24.652	20.975
30%	79.25	77.907
40%	109.87	105.236
50%	195.296	188.581
60%	370.91	365.89
70%	445.85	436.89
80%	548.03	543.14
90%	704.85	693.27
100%	1.68E+03	1.70E+03

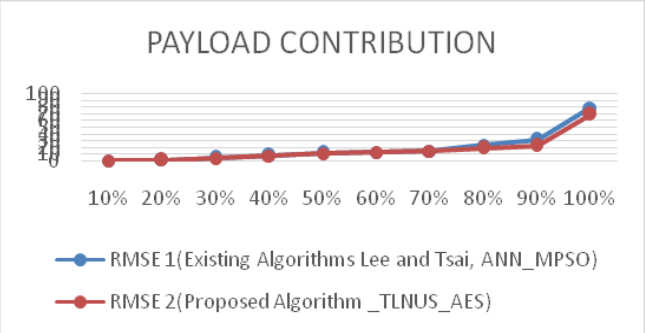

Figure 10 Payload Contribution for two algorithms using RMSE metrics

VIII. CONCLUSION

This research paper solved the problem of embedding all types of data of maximum size of 0.9910 accuracy presented in cover image by upholding robustness and quality of images. Finally authors designed hybrid algorithm which convey three inner contents like text,image and audio could accommodate in cover original image without disturbing authentication and integrity.

In the future work, the current secure framework is extended to adding video content inside an image to be implement for further future.

An introduction to the data hiding techniques is followed by a study on Text hiding, Image hiding and audio hiding in digital image envelope. A critical survey[14-19] on Watermarking, fingerprinting, cryptography, steganography techniques. its characteristics, applications deployment processes for the hybrid steganography technique is presented. The importance of data hiding is given. Data sets are being used[7][9][10] for the experimentation as mentioned in a detailed fashion. Then a detailed study on two baseline systems is provided along with the results.Several hiding techniques [7] were investigated in order to identify means to improve the system's robustness and flexibility to handle multimedia data to hidden effectively. It was found that a TLNUS model based on three layer protection hiding techniques is reduces the number of layers in existing algorithms and also improve hiding quantity up to 39 % of payload contribution. Further, it was found that hiding audio in image did not contribute any significant work to the system. Then we presented the way to deal with audio samples of mp3,wav data set in case of data hiding in cover images. Here we considered Key based position system, to hide content of audio samples using sampling theory and apply conversion of audio samples upto 37% into binary as well as testing. For linking we used pivot element of green color of every color image data set considered is i-1,i, i+1 format[62].

Using the phenomenon from the wav files we can fit the redundant places of cover image. To achieve this task, we have come up with a new procedure where audio samples were encoded into cipher form using AES algorithm. When the proposed data hiding algorithms was implanted as a part of this assessment of quality of image, the results surpassed the efficiency of conventional methods.

ACKNOWLEDGEMENT

We owe our tributes to Dr.R.Sivaranjani, Head of Department, ANITS for all his support in technical aspects and for his guidance.

REFERENCES

1. F. Johnson,Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", publised in IEEE, 1998, pp 26-43.
2. jagadish, P sanyasi naidu, published paper "Scalable Methodology to Hide Audio Data in Cover Image using RGB and Gray Color based Key Positioning Image Steganography",IJRTE, ISSN: 2277-3878, Volume-8 Issue-3, September 2019.
3. Moni Naor and Adi Shamir, “Visual cryptography. in Proceedings of Advances in Cryptology”, EUROCRYPT 94, LNCS Vol. 950, pages 1-12. Springer - Verlag, 1994.
4. P.Sanyasi Naidu, J Gurrala “Investigation and analysis of Location Based Authentication and Security Services of Wireless LAN’s and Mobile Devices”, published in IJCA ,Volume 146,Number 8 (ISBN: 973-93-80893-84-7 , July2016.
5. W Bender, “Echo Hiding", D Gruhl, A Lu, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 295-315.
6. Nameer El-Emam., et al, "New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization”, Elsevier 2015, computers & security 55 (2015) pp21–45.
7. A. Cheddad, J. Condell, K. Curran, & P. McKevitt, “Digital image steganography: survey and analysis of current methods”, Signal Processing, 90(3), 727-752, 2010.
8. El-Emam, N., Al-diabat, M., “A novel algorithm for colour image steganography using a new intelligent technique based on three phases,” Applied Soft Computing, Vol. 37, pp. 830–846, 2015.
9. J Gurnsey, Aslib Gower, “Copyright theft”, IEEE, 1995.
10. Akhshani A, Akhavan A, Mobaraki A, Lim S, Hassan Z. "Pseudo random number generator based on quantum chaotic map" Commun Nonlin Sci Numer Simul 2014;19(1):101–11. doi:10.1016/j.cnsns.2013.06.017.
11. Ali L, Aris I, Hossain F, Roy N. Design of an ultra high speed AES processor for next generation IT security. Comput Electr Eng 2011;37(6):1160–70. doi:10.1016/j.compeleceng.2011.06 .003.
12. Bedi P, Bansal R, Sehgal P. Using PSO in a spatial domain based image hiding scheme, with distortion tolerance. Comput Electr Eng 2013;39(2):640–54. doi:10.1016/ j.compeleceng.2012.12.021.
13. Beheshti Z, Shamsuddin S, Hasan S. MPSO: Median-oriented Particle Swarm Optimization. Appl Math Comput 2013;219(11):5817–36. doi:10.1016/j.amc.2012.12.013.
14. Cetin O, Ozcerit A. A new steganography algorithm based on color histograms for data embedding into raw video streams.Computers & Security 2009;28(7):670–82. doi:10.1016/ j.cose.2009.04.002.
15. Qian Z, Zhang X. Lossless data hiding in JPEG bitstream. J Syst Softw 2012;85(2):309–13. doi:10.1016/j.jss.2011.08.015.
16. Qin C, Chang C, Liao L. An adaptive prediction-error expansion oriented reversible information hiding scheme. Pattern Recognit Lett 2012;33(16):2166–72. doi:10.1016/ j.patrec.2012.08.004.
17. Qu Z, Chen X, Zhou X, Niu X, Yang Y. Novel quantum steganography with large payload. Opt Commun 2010;283(23):4782–6. doi:10.1016/j.optcom.2010.06.083.
18. Rabevohitra FH, Sang J. High capacity steganographic scheme for JPEG compression using particle swarm optimization. In Proceedings of International Conference on Material Science and Information Technology,Volume 433–440, Singapore; 2012, 5118–22. doi:10.3844/jcssp.2007.223.232.
19. RG van Schyndel, AZ Tirkel, "A Digital Watermark", CF Osborne, in International Conference on Image Processing, (IEEE,1994) v 2 pp 86-90.
20. P Wayner, "Disappearing Cryptography| Being and Nothing on the Net', AP Professional (1996).

AUTHORS PROFILE

Mr.G.Jagadish, currently pursuing Ph.D from GITAM, deemed to be university since 2014 under the esteemed guidance of Dr.P.sanyasi Naidu. He has received his Masters’ in Computer Science & Technology- specialization in computer networks from CSSE in 2009, Andhra University. He is currently working as Assistant Professor in Anil Neerukonda Institute of Technology & Sciences, Visakhapatnam since 2009. He has an excellent command on programming in C,C++,java, network security, steganography and presented many papers internationally. He is the currently member of ACM- 7008666.He passed online certification in Secure system engineering under Information Security, through NPTEL course.

Dr. Pasala Sanyasi Naidu, received doctorate in Computer Science Engineering from Andhra University in the year of 2011. He is currently working as a Associate Professor in Department of Computer Science and Engineering Department at GITAM deemed to be University since 2001. He got Best performer award in the year of 2010 in teaching. His main interests lie in Image Processing, Computer Networks, Network Security, Cryptography, Formal Languages Automata Theory, C, Java. He is a life member of Indian Society for Technical Education. He is published 43 national and international journals and conference in his strength.