Hybrid Steganography Model for Secured & Efficient Data Transmission on Computer Networks

[1]Shaik Aashiq, [2]C. Madhu
[1] IV B.Tech Student, Dept. of ECE, S V College of Engineering, Tirupati, India;
[2]Asst. Professor, Dept. of ECE, S V College of Engineering, Tirupati, India;
[1] shaikaashiq98@gmail.com [2]cherukulamadhu@gmail.com

Abstract: **Advancement of data and correspondence Technology expanded the necessity of protection and security. A huge data is in the public shared media. The requirement of security to this data leads to rapid development of the cryptographic Technique. Steganography is the science of concealing secret information in media files (i.e., image, text, audio, protocol, etc.), so that, such information is not perceptible by an eavesdropper. There are numerous methods used to shroud mystery data to accomplish high caliber of stego Image and high inserting limit. There are numerous difficulties in steganography including the endeavors to uncover mystery data that has been covered up. So many researches and workouts were done to develop a lot of techniques and algorithms to find solution to this problem. This project proposes a method for hiding the secret image, in another image nothing but cover image, using more than one algorithm.**

Keywords: **Steganography, Encryption, Stream Cipher, ASCII based Encryption, LWT Compression, Secured data transmission.**

I. INTRODUCTION

The word "Steganography" can be interpreted as "hidden writing". Steganography was firstly used by Ohannes Thritemeous in his book "steganography". The major intention is to hide the secret information in media, so that only authorized persons can see it [Richard, 1998]. The following gives the fundamental process of steganography.

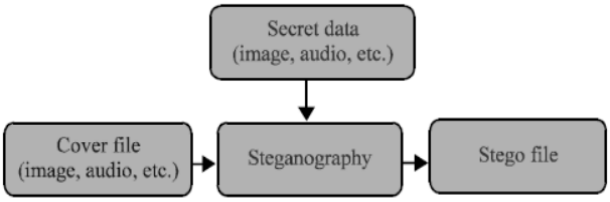

Fig 1. Fundamental Process of Steganography

Steganography based on text: This technique uses normal text to hide secret information. This classical method of hiding the information is considered as an important method of hiding. Also, this approach is considered efficient since a normal text file contains less redundant information [1].

Steganography based on audio: This technique uses audio files as cover files to hide the information.

Steganography based on image: This technique uses images to hide the secret information. In addition to that hiding information in digital images is one of the most popular ways for several reasons. Digital images contain a lot of extra bits that can be replaced with secret data without any difference between them and the original image. The increasing use of digital images in digital media and the internet, particularly social media. Furthermore, there are 2 types of image steganography techniques in this area:

1. Spatial domain, where secret data will be implanted directly in the intensity of pixels.
2. Transform domain/ frequency domain, here images are first transformed and then secret information is embedded in the image [2; 3].

Likewise there so many ways of steganography, but this article mainly concentrates on image based steganography.

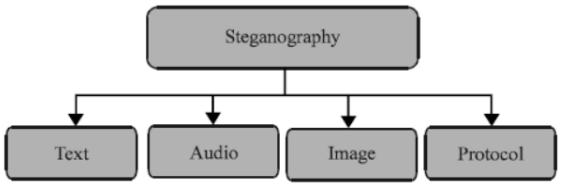

Fig 2. Types of Steganography based on cover file

Also, types of steganography techniques can be lassified based on hiding methodology as shown in the figure.

This paper concentrates on image based steganography that too in transform domain based hiding technique and it is manly divided in to two parts as follows

Firstly, the work concentrates on the secret image or secret data, which means first the secret image/data will be processed to reduce the bandwidth or data rate, so that more data can be incorporated on the cover image.

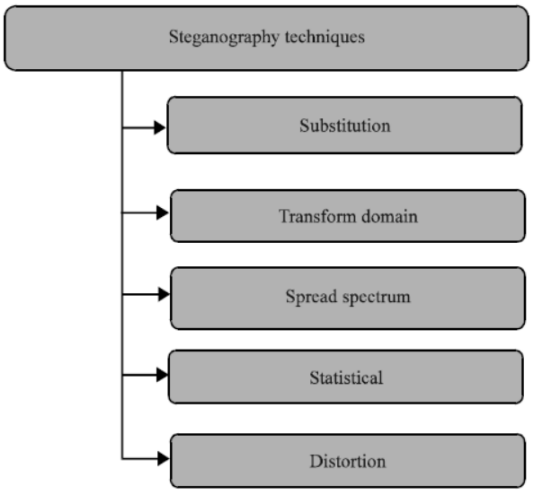

Fig 3. Types of steganography based on hiding method

For that, initially a compression algorithm was implemented; this compression is done with Discrete Wavelet Transform (DWT). Then with the thought of improving the secrecy, an encryption algorithm or cryptographic algorithm will be

implemented on the compressed image. Because of this both entropy and privacy will increase.

Secondly the embedding process will be done with the help of Lifting Wavelet Transform (LWT), to embed the secret data in to various sub-bands of the cover image.

ASCII based stream cipher will be used for encryption to increase the robustness and security as it acts much better than that of Rivest – Shamir –Adleman (RSA) algorithm, which was existing method. Certain quality metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) also compression Ratio (CR) have been used to calculate the quality of this model.

II. Processing (Compression) of Secret Image

This procedure manages the fundamental necessities like information rate and capacity limit of a framework while changing over simple information to computerized information. These necessities can be accomplished by compacting the information. There are number of picture pressure strategies, yet this paper focuses on Set Partitioning in Hierarchical Trees (SPIHT), which is a wavelet based pressure calculation that offers great pressure proportions, completely dynamic piece stream and great picture quality. This paper exhibits the aftereffects of adding number-crunching pressure to the SPIHT pictures with expectations of further decreasing the picture estimate with better information rates and picture quality.

SPIHT joined with Huffman Encoding (SPIHT-HC) strategy to decrease redundancies [4] has bring down pressure proportions and sets aside much time for encoding and unraveling process. Since, Huffman encoder encodes every image in the arrangement independently. In this way, there is a need to enhance these parameters for productive pressure and transmission of information. We have exhibited therapeutic picture pressure calculation by joining SHIPT with number-crunching coding. The square chart for proposed calculation i.e. medicinal picture pressure is appeared underneath in figure.

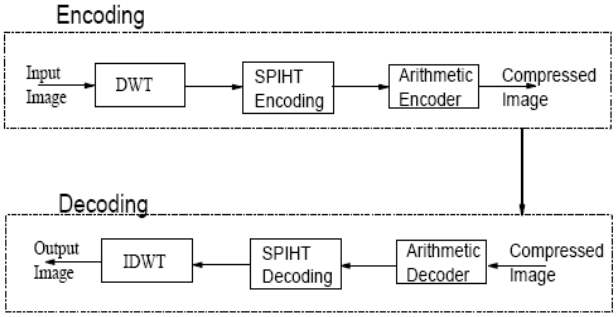

Fig 4. Block Diagram for image compression using SPIHT combined with Arithmetic Coding

Set Partitioning in Hierarchical Trees- Description

SPIHT is an implanted coding method, where installed coding calculations, encoding of the flag at lower bit rate is inserted toward the start of bit stream for the objective piece rate. Picture information through the wavelet disintegration, the coefficient of the dissemination transform into a tree. As indicated by this component, a spatial introduction tree would be shaped by characterizing an information structure. 4-level wavelet decay of the spatial introduction tree‟s structure are appeared in Figure 2.We can see that every coefficient has four kids with the exception of the „red‟ checked coefficients in the LL sub-band and the coefficients in the most elevated sub-groups (HL1;LH1; HH1).

Set Partitioning of Hierarchical Trees with Arithmetic Coding (SPIHT-AC)

For the yield bit stream, SPIHT encoding with an extensive number of seriate "0" circumstance, we get a determination by a ton of factual examination: „000‟ shows up with the best likelihood esteem, generally will be around 1/4. Along these lines, separate the double yield stream of SPIHT each 3 bits as a gathering.

Each gathering recorded as an image, an aggregate of eight sorts of images, likelihood that they show up and after that encoded utilizing entropy coding normally achieved the further packed in proposed framework. (Number juggling coding is utilized as an entropy coding). Number-crunching coding is a notable technique for lossless information pressure [5,6]. The thought can be followed back to crafted by Shannon [7], yet it was first unequivocally depicted by Elias and portrayed as a commentary in reference [8].

Number-crunching coding is a pressure procedure that can give pressure levels at (or) close entropy. What it implies is that in the event that we have a message made out of images over some limited letter set, we can produce the correct number of bits that relates to an image (e.g. 1.6 bits/image).

This is restricted in Huffman encoding which must yield a whole number of bits per image (e.g. 2 bits/image). Number juggling coding accomplishes entropy (or extremely close it) by gathering images together until the point that a whole number estimation of bits can be a yield for a succession of images (e.g. ABC may compare to 1011).

III. Encryption of Compressed Secret Image

With the increased usage of the internet, Due to popularity of e-commerce applications and social networks, a large amount of data is transferred on the networks daily. Providing security to this Data is the utmost critical issue. Ensuring safe transmission of information through the internet is much needed. Issues related to network security are most important now because society is moving towards digital information age. As usage of internet is increasing it attracts a lot of cyber-criminals [9].

Cryptography is a Technique to provide security to the Data. It is the process of conversion of data into the secret code with the help of key .This data can be converted to original form by only authorized person using a key again. This called cryptographic process. Converting the original data to coded form is encryption and conversion of coded form to original form is called decryption.

Based on number of cryptographic keys used for encryption and decryption cryptographic keys are categorized [10].

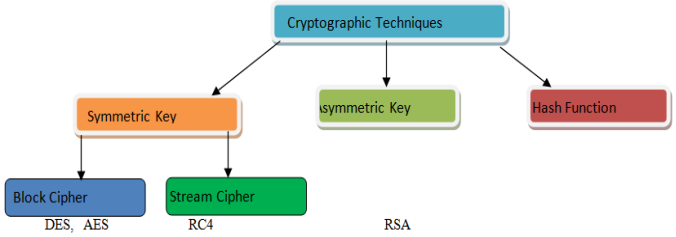

Fig 5. Different Cryptographic Techniques

4.3 Proposed cryptographic technique using ASCII

Encryption:

Step1: Read each character of plain text, find out corresponding ASCII value and store it in InputArray
Step2: Read the secret code in array S convert each element of array S into seven bit binary
Step3: Calculate 2's compliment of binary sequence obtained in step2
Step4: Add 8 bits to the left side of value in step2. Now convert it into 8X8 matrix 'X'.
Step5: Add 8 bits to the left side of value obtained in step3. Convert it into 8X8 matrix 'Y'.
Step6: Z=XY.
Step7: Add elements of Z and store the result in 'A'. If sum is zero assign secret value to 'A'. If sum is greater than 127 then A=A mod 127. Convert A to seven bit binary and repeat these 7 bits to obtain length equal to length of input. Store it in array I. split Iinto two arrays I1 and I2 so that I1 consists of element from sum to end of I and I2 consists 0 to sum-1.Now concatenate I1 and I2 to get single array S1.
Step8: perform XOR operation between this S1 and binary form of input array. Convert the result into decimal values considering seven bits at a time and corresponding sequence of ASCII characters are cipher.

Decryption:

Step1: Read each character of cipher text, find out corresponding ASCII value and store it in OutputArray
Step 2: Read the secret code in array S. convert each element of array S into seven bit binary
Step 3: Calculate 2'compliment binary sequence obtained in step2
Step4: Add 8 bits to the left side of value in step2. Now convert it into 8X8 matrix 'X'.
Step5: Add 8 bits to the left side of value obtained in step3. Convert it into 8X8 matrix 'Y'.
Step6: Z=XY.
Step7: Add elements of Z and store the result in 'A'. If sum is zero assign secret value to 'A'. If sum is greater than 127 then A=A mod 127. Convert A to seven bit binary and repeat these 7 bits to obtain length equal to length of input. Store it in array I. split I into two arrays I1 and I2 so that I1 consists of element from sum to end of I and I2 consists 0 to sum-1.Now concatenate I1 and I2 to get single array S1.
Step8: perform XOR operation between this S1 and binary form of OutputArray. Convert the result into decimal values considering seven bits at a time and corresponding sequence of ASCII characters are plain text.

IV. Embedding in Transform Domain via Lifting Wavelet Transform (LWT)

Lifting Wavelet Transform is similar to DWT except that the number of samples at each stage is same as the initial set of samples. The input samples are split into odd and even sets of samples and passed through the filters (lifting steps) to give rise to approximation and details. Since the number of samples to be stored is same as that of the input at each stage, we can save memory. The number of computations required is also reduced, since the approximation coefficients at one level can be derived from the detail coefficients already computed and some of the input samples [11]. The integer wavelet coefficients are also possible with perfect reconstruction [12]. Lifting Wavelet Transform provides ease in implementation in hardware.

LWT reduces to the poly-phase version of the DWT algorithm with zero-padding extension mode and without extra-coefficients.

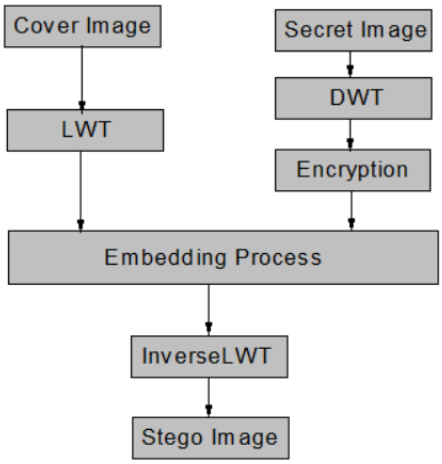

Fig 6. Block Diagram for Embedding Stage in Proposed Steganography

V. Results & Discussion

To evaluate the efficiency of the proposed model a number of experiments were done and are shown in the following tables: Table 1 shows the secret image's Mean square error (MSE), peak signal to noise ratio (PSNR) and compression ratio (CR). While table 2 shows the cover images, secret images and stego image and PSNR, MSE. The following test images were used as cover and secret images.

Fig 7. Cover Images for testing the algorithm

Fig 8. Secret Images for testing the algorithm

The results for the proposed algorithm are shown in the following figure and tables.

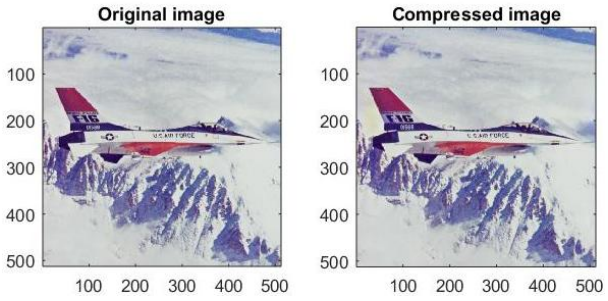

Fig 9. Results of Compression algorithm

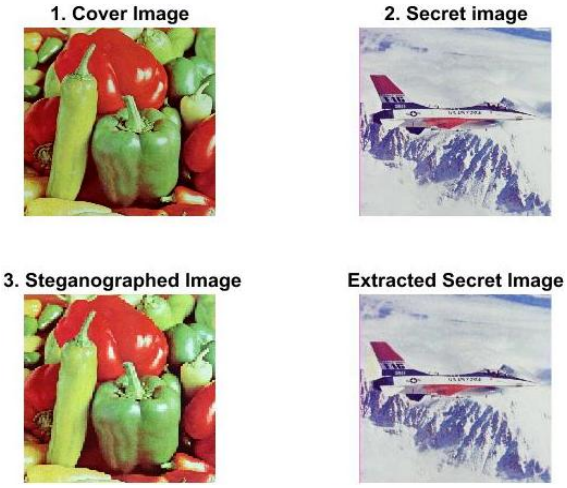

Fig 10. Results of steganography

Table 1: Performance evaluation of Compression Algorithm for DCT & DWT

S.No.	Method	Compression Ratio	Mean Square Error	Peak Signal to Noise Ratio
1	DWT	34.8404	2.5715	44.0290
2		51.1042	2.3852	44.3556
3		37.3001	1.1196	47.6403
4		49.8099	3.1185	43.1914
1	DCT	9.2871	30.6228	33.2704
2		14.2902	33.4726	32.8839
3		10.0302	22.5553	34.5983
4		11.4880	30.4286	33.2980

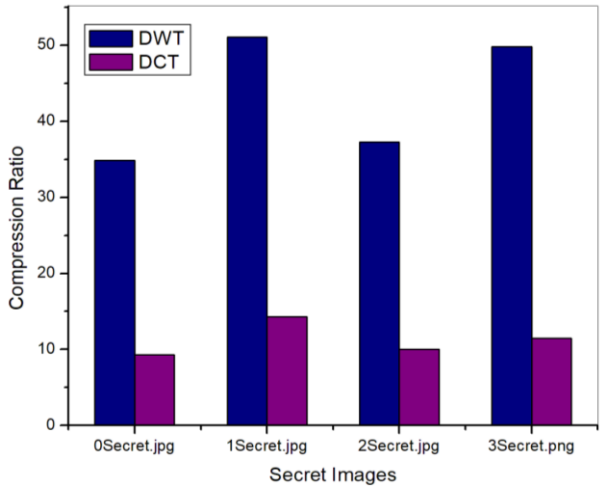

Fig 11. Compression Ratio Comparison

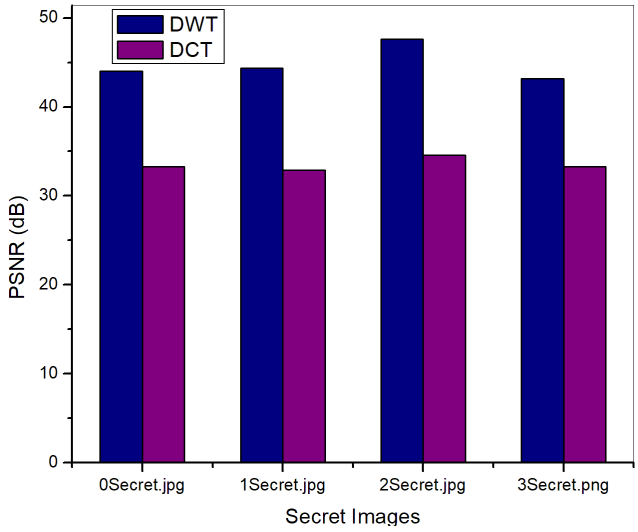

Fig 12. PSNR Comparison during Compression

Table 2: Performance evaluation of Steganography Algorithm for DWT & LWT

S.No.	Method	Mean Square Error	Peak Signal to Noise Ratio
1	DWT	59.8372	30.3951
2		63.8171	30.1154
3		193.0374	25.3084
4		34.1306	38.8540
1	LWT	59.1626	30.4443
2		64.2786	30.0841
3		192.6645	25.3168
4		33.9782	38.8734

CONCLUSION

The Proposed model of hiding the data i.e, by using hybrid steganography, nothing but steganography followed by cryptography outperforms the classical steganography method. As discussed earlier this model is divided in to 2 stages. The first

stage is the embedding stage. The second stage is the extraction stage. In this paper, the main aspects of the success of steganography model were taken in to considerations (capacity, security, robustness). To evaluate the proposed method few parameters were calculated, and those are PSNR, MSE, and CR. The extracted secret image is similar to the original confidential image. And we can say that this model provided the following:

- This model provides more security due to the usage of cryptographic algorithm.
- Using the DWT algorithm provides more space for hiding secret image.
- The lifting wavelet transform provides robustness for steganography process.

REFERENCES

[1] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).

[2] Juneja & Sandhu 2009, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," in proceedings of International conference on Advances in Recent Technologies in Communication & Computing. DOI:10.1109/ARTCom.2009.228

[3] Ali, B.K.S.M.H. and A.B. Kadhim, 2016. An efficient steganography mpdel using video compression and imge steganography. J. Babylon Univ. Pure Appl. Sci., 24: 1145-1154.

[4] Wei Li, Zhen Peng Pang and Zhi Jie Liu, "SPIHT algorithm combined with Huffman encoding" in Third International Symposium on Intelligent Information Technology and Security Informatics, 2010 IEEE Trans. vol.26, pp.341–343.

[5] Ian H. Witten, Radford M. Neal, and John G. Cleary, Arithmetic coding for data compression. Communications of the ACM, 30(6):520-540, June 1987.

[6] Glen G. Langdon Jr., An introduction to arithmetic coding. IBM Journal of Research and Development, 28(2):135-149, March 1984.

[7] C. E. Shannon, A mathematical theory of communication. Bell System Technical Journal, 27:379-423 and 623-656, 1948.

[8] Normand Abramson, Information Theory and Coding. McGraw-Hill Book Company, Inc., New York, NY, 1963.

[9] Shyam Nandan Kumar, "Review on Network Security and Cryptography." International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 1-11. doi: 10.12691/iteces-3-1-1.

[10] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, VOL. 2, Issue 7 July 2012, Page 226-233.

[11] C.Valens, *The Fast Lifting Wavelet Transform*, A tutorial.

[12] A.W.CalderBank, I.Daubechies, W.Sweldons, *WaveletTransforms That Map Integers to Integers*, Applied and Computational Harmonic Analysis, Vol. 5, no. 3. pp.332-369, July, 1998.

About the Author(S)

Mr. Shaik Aashiq, pursuing IV B.Tech in the department of ECE, S V College of Engineering, Tirupati, India, is very much interested in research area that too in digital image processing inspired by current advancements in the same area, he's a student member in IETE student forum and acted as student chairman during 2017-18 academic year.

He organized few technical events at college level in collaboration with familiar organizations like unity India and secured certifications from Google Academy and Mathworks for completion of Analytics individual qualification and self paced courses in MATLAB and Deep Learning respectively. He also worked on Arduino based kits to improve his technical knowledge.

Mr. C. Madhu, working as an Assistant Professor in the department of ECE at S V College of Engineering, Tirupati India, Completed his post graduation at Sri Venkateswara University College of Engineering, Sri Venkateswara University, Tirupati in 2011 and completed his UG at Siddharth Institute of Engineering and Technology, Puttur, Affiliated to JNTUA, in the year 2009. He is a life member in ISTE, IAENG and SDIWC

He has published 15 articles in international journals and 2 articles in national journals and presented few papers in nation and international conferences in the area of Signal and Image Processing.