DESIGN AND ANALYSIS OF A REVERSIBLE STEGANOGRAPHY USING LSB BIT SHIFTING ALGORITHM

SONGA PRATHAP [#1] , K.VENKATA RAO [#2]

[#1] M.Tech Scholar,Department of Computer Science and Systems Engineering, College of Engineering,Andhra University,Visakhapatnam,AP,India.

[#2] Professor,Department of Computer Science and Systems Engineering, College of Engineering,Andhra University,Visakhapatnam,AP,India.

ABSTRACT

Now a day's security has become one of the challenging problems in almost all fields like IT, Banking, Medical, MNC companies and many more. As security plays a vital role, in order to provide security for the normal text data or sensitive message which is to be transferred over network is achieved with the help of cryptography algorithms. This has achieved high level of security for the text data, but failed to provide security for the digital data (I.e. Audio/Video/Images) in any manner. So at this stage there is a new concept which came into existence that is steganography, which means hiding one form of data within other rather than converting one form to other. Steganography is a new branch of security through which one form of data can be hidden in another form of data of either same type or of different type of formats. This new mechanism is mainly implemented in order to provide much more security for digital data which is to be sending over network. As the user regularly transfer a lot of files from one system to other system either within the range or far range by using internet or intranet, he eventually looks for more security. This paper helps to analyze how to send a file from one place to another in a secured manner. Firstly the target file is encrypted using our primitive cryptography algorithm called as DES Bit Shifting and it is embedded into an audio or video or any media file. For embedding one file within other we use LSB (Least Significant Bit) Algorithm for hiding one form of data within the other and we also use the texture synthesis method in which the text or message can also be embedded with any of the digital data. The resultant file will be protected by a password. This resultant media file has no change in its original format and it can be run in any player without affecting its original quality, we can't find any encrypted data inside it. This format will be sent through Internet or through any form of wired communication networks. Once the receiver receives the carrier file from sender through any form of network either LAN or Internet, he will then use the same software to retrieve the hidden data from that carrier file. By conducting various experiments on our proposed reversible steganography methods, we finally came to a conclusion that this reversible texture synthesis gives much more security for the digital data in terms of efficiency, integrity and many other ways compared with the primitive steganography algorithms.

Key Words: Secure Communication, Sensitive Data, Embedding, Encryption, Carrier File, Master File.

I. INTRODUCTION

In present day's communication of valuable digital data (I.e. Image, Video, or Audio) through public or un-secured channels have become a most critical problem in the society. This major problem is solved by using the new concept called steganography, which is the art and science of hiding valuable information into Master channels so as to conceal the information and prevent the detection of the hidden message. Steganography is also defined as hiding information within a noise; a way to supplement (not replace) encryption, to prevent the existence of encrypted data from being detected [1] by the un-authorized users. According to Greek literature ,steganography is also known as "covered writing method", a branch which deals mainly with only two methods like Embedding and De-Embedding of original valuable content within a Cover file like image, video, or audio[2],[3],[4]. This new technique is mainly used by the Indian Government in the Military to establish relationship between more than two military commanders in a much secured manner without releasing or misusing any small part of embedded data [5], [6].

Although there was a various security primitives that are available in the literature, if we go with all the literature steganography has been used as a secure means to hide the sensitive information securely and communicate them in a secure manner. In olden days there are some primitive methods that were widely used for sending the information securely to the receiver nodes, they are as follows:

1. Invisible Ink Method
2. Writing on Shaved Heads Method
3. Microscopic Images Method

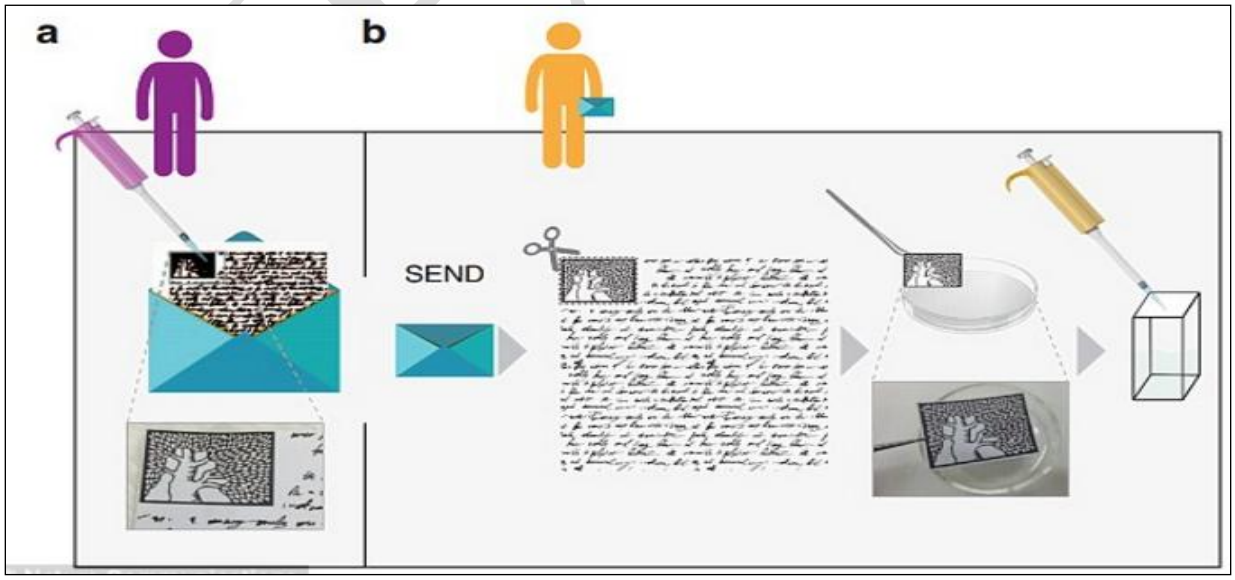


Figure 1. Represents the Invisible Ink Method for Sending data Securely over Network Channel

From the figure 1, we can clearly get an idea that there are two users named ‘a’ and ‘b’ who try to send the information securely over network, so that the user ‘a’ try to apply invisible ink method for sending that valuable message to the receiver ‘b’.Once the sender sends the message in this format over network no other person who is available within the network can able to easily view the content, even if they try to hack the content illegally. So the receiver can only receive the data in a secure manner and he can follow the reverse process to decrypt the data into a visible manner.

Working Principle of an Steganographic System

We can clearly find the advantages of steganography mechanism from the working principle diagram from the below figure .2, which clearly states the description about an embedded data either text/audio/video/image inside any digital media like audio/video/image type data, so as the data which is passed through the carrier file cant able to identify or open by any un-authorized users who wish to access the data. So in this paper we clearly explain the advantage of new novel steganography concept under mixed category of how one type of digital media data is embedded within other type of digital data either of similar type or different type formats by giving password for the embedded data.

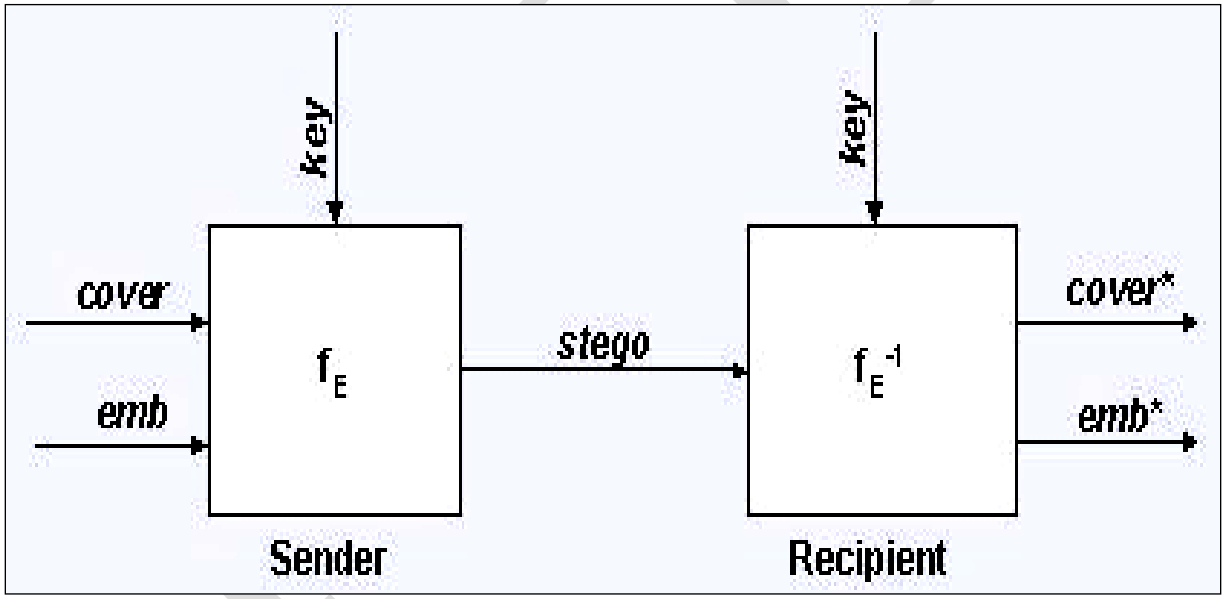


Figure 2. Represents the Working Principle of an Steganographic System

Where the function

fE **:** Which clearly denotes steganographic Function for embedding.

$\mathbf{f_E^{-1}}$: Which clearly denotes steganographic function for extracting of hidden data.

Cover File: This is the main source file in which the sensitive data will be hidden.

Emb Function: This is the important function in our process which indicates message to be hidden.

Key Function: Which is a new Parameter of f_E

Stego Function: This is a function which denotes the data that has both cover data with hidden data.

In this current paper, we are not following the primitive cryptographic encryption and primitive cryptographic decryption techniques. We are introducing a novel cryptographic algorithm called as Novel Bit Shift encryption in Random Cycle Order. I.e. totally 4 different types of Bit Shift algorithms are used randomly to encrypt the data like 4-Bit,6-Bit,12 Bit ,16 Bit Shift Encryption Algorithms. This Encryption is embedded into an Image or Audio or Video File. Again it will be embedded into a media data. This means initially we will choose any digital file either image or audio or video and we try to hide the valuable sensitive data inside that file and in turn save the carrier file with a own file name as a output file. Now this output file will actually contains multiple data like sensitive data and the password to de-embed the hidden file, hence it is very secure to send and access over the network. Also the password protection for the data in this proposed work gives an additional security for this total application, if there was no password facility the user may lost the valuable data in the terms of intruders between data transmission.

II. BACKGROUND KNOWLEDGE

In this section we will mainly discuss about the background work that was carried out in order to implement this reversible texture synthesis over digital data. Now let us look about some of the preliminaries or real time applications where the steganography technique is used.

A) Steganography on Text Data

In this section we will mainly discuss about the advantage of applying steganography on text formats, now let us look about that in detail as follows:

Steganography is a Component suite that can be used as a component in any application to provide the security to the text file. Steganography provides several functions.

It will take the TEXT file and password as input and gives the Encrypted and embedded audio/video/image file as output.

It will take the password and embedded audio/video/image file as input and will give decrypted and original TEXT file.

Functional requirements for the promised text based security system are as follows:

Expected Inputs:

File Details: The input file should be of Digital File (I.e. Either Audio/Video/Image file).

Text Details: Here the message will be stored in a text file

Here in the above file details we have mentioned the input file type as audio/video/image file where the input data can be of any type and the text details indicates the type of data that is used for hiding. As per the current survey we will take any type of text documents or .java files for hiding inside the file type.

Expected Outputs:

Audio/Video/Image Details: Embedded audio/video/image

Text Details: Original Text file or Text message

Storage Details:

Cipher text generated from plain text

Cipher text extracted from Audio/Video/Image file.

Generating cipher text: Using the DES algorithm the cipher text is generated.

Hiding the cipher text in audio/video/image: Using low bit encoding method the cipher text is kept hidden in the audio/video/image file.

B) Data Encryption Standard Algorithm

Data Encryption Standard (DES) algorithm is one of the best algorithm in cryptography, where this is used to encrypt the data securely with a password and make the data into invisible manner. As we are using the DES algorithm for giving security for the embedded data, the password should be always not less than 8 characters and DES algorithm uses 64 bit key size for implementing the keyword. We also know that DES algorithm comes under symmetric key encryption algorithm, the sender and receiver must submit the same keys in order to encrypt and decrypt the hidden file from an embedded file[8]-[10].

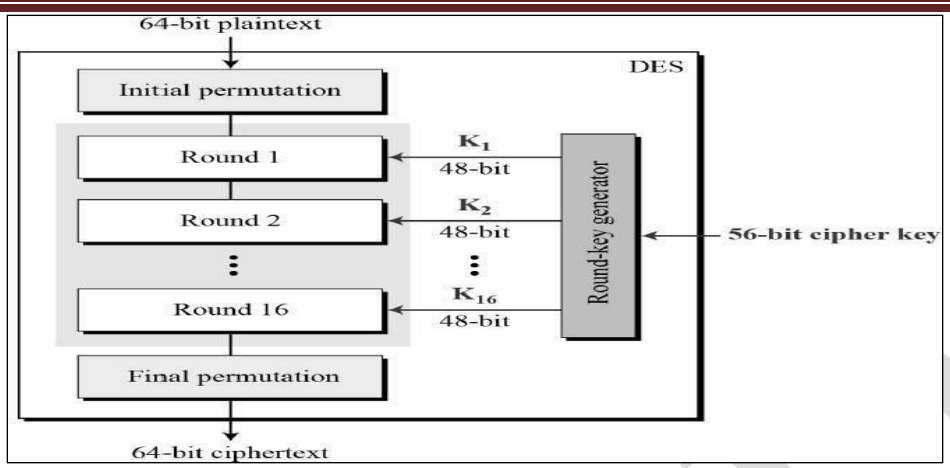


Figure 3. Represents the Architecture of DES Algorithm for Encryption

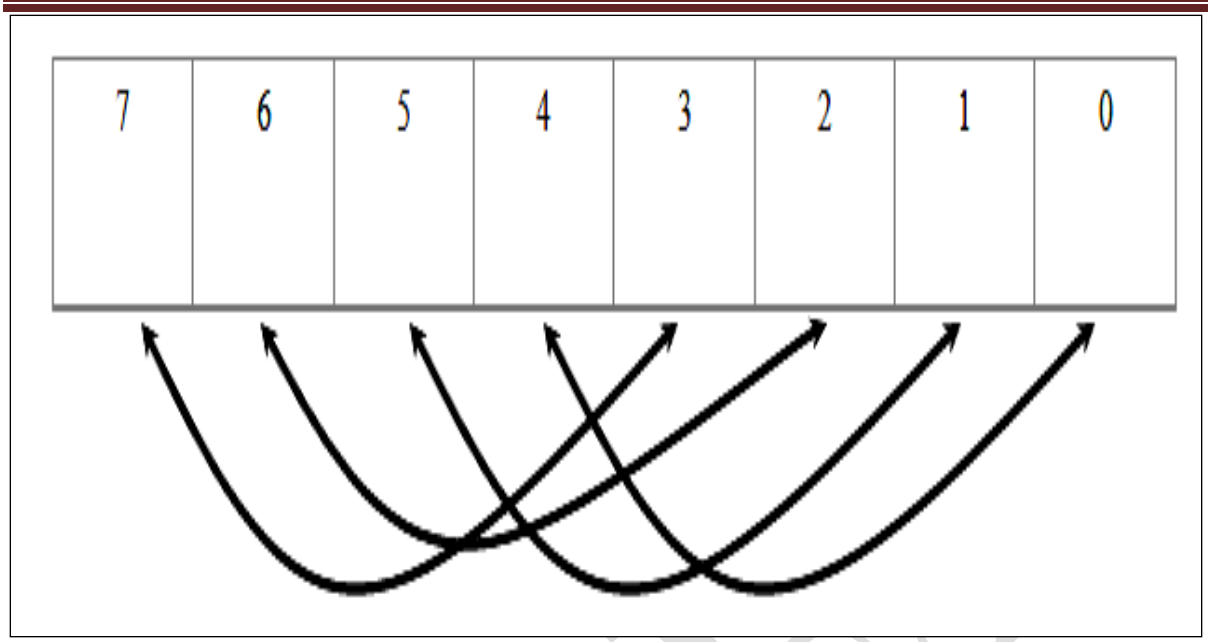
As we all know that DES algorithm is a symmetric encryption algorithm as shown in above figure 3, the sender and receiver should substitute the same key for encryption and decryption at both the ends. Initially we take 64 bit plain text as input we undergo the initial permutation for the 64 bit plain text the permutation starts with round 1 and it will keep on incremented and finally it is terminated at round 16, where that is the final round in our DES algorithm. During this iteration there will be generating a 56 bit cipher key with a key sizes of 48 bit during all the 16 rounds. Once all the 16 rounds were completed, the plain text will be automatically converted as cipher text of 64 bit size [12].

III. BIT SHIFT TRANSFORMATION APPROACH

In this section we mainly discuss about the bit shit transformation approaches that are widely used in our proposed paper. Now let us look at them in detail:

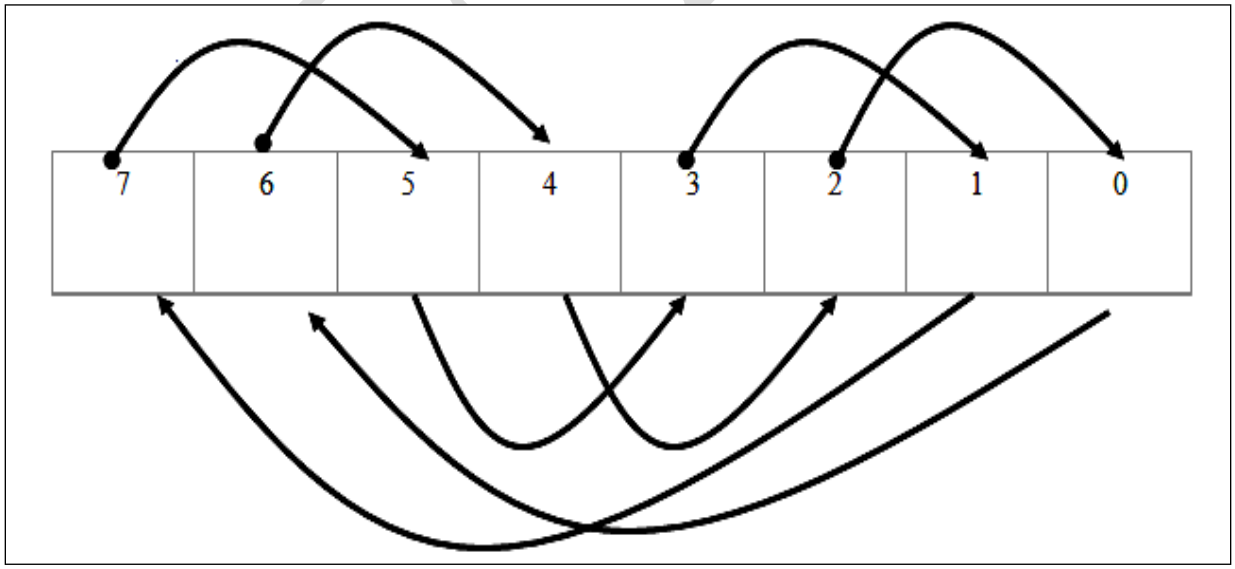
This was the second steganographic technique which was used in order to give more security for the data by applying bit shift operation. There are several types of Bit Shift Operations like 2-Shift, 4-Shift, and 6-Shift and so on. We apply four Bit-Shift operations in the current application in order to give more security by applying these transformation techniques.

Bit Position



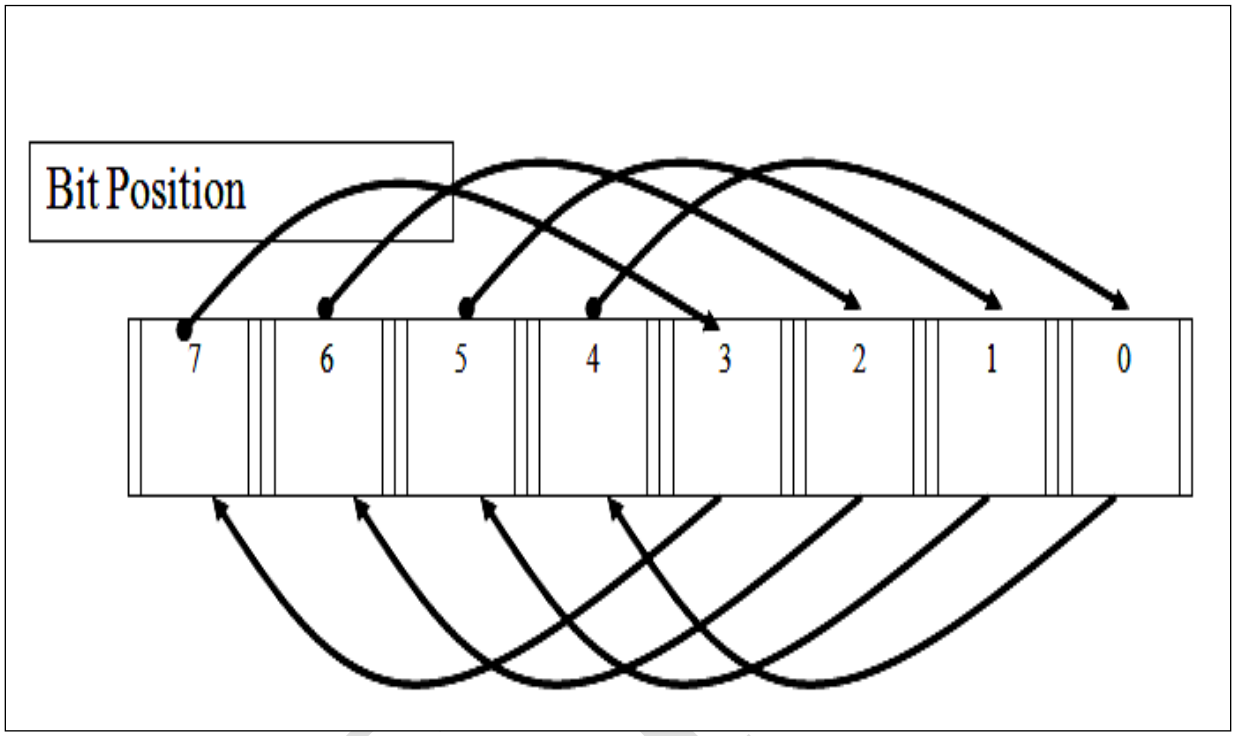
Shift Algorithm – 4 Shift

The above is the 4 Bit transformation approach which is used for shifting 4 bit positions from left to right, starts from the middle bit position. And this

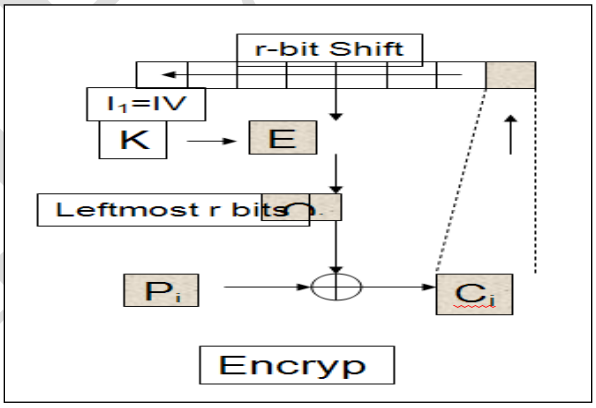


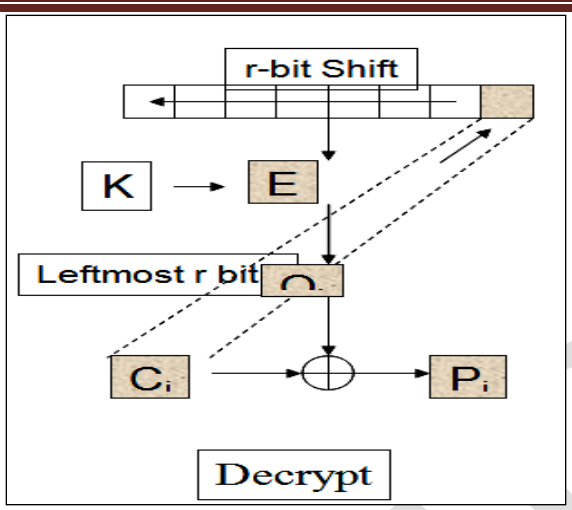
Shift Algorithm – 6 Shifts

The above Bit Position clearly indicates it is an 8 bit string with change of 6 bit positions from left to right side. In the same way we can do continue with remaining other bit positions like 12 and 16 bit positions.



Bit Shifting – Encrypt & Decrypt





From the above two figures we can clearly get an idea that encryption and decryption process with bit shifting. Here the encrypt and decrypt are done with leftmost r bit shift.

IV. PROPOSED REVERSIBLE STEGANOGRAPHY TECHNIQUES

In this section we will mainly discuss about our proposed reversible texture synthesis and various steganography techniques that are used in the proposed paper. Now let us discuss about them in detail as follows:

In the current days there is a lot of user attention towards the data hiding techniques in almost all fields especially in the field of IT. The main reason why this has gained the popularity is because there is a fear like encryption services are getting outlawed. There are several ways to hide information in digital data like image, video or audio type of any formats. We look at the one of the most important approaches:

Now let us look at the one of the best approach in detail as we are using this approach for our proposed paper. Before we go directly into the main topic like LSB insertion, we analyze some of the important properties of steganography that are used in the current LSB insertion algorithm. Generally there are several important factors required to perform the steganography, of all the factors two are most important. They are as follows:

i) The Cover File
ii) The Data File

The cover file is the medium into which we will embed the data. In the steganography choosing an appropriate cover file is an important decision, as it is a large part of what determines the effectiveness of the steganographic technique. Steganography's mainly relies on 'hiding' the sensitive data behind the cover file and prevents it from being considered secure, unlike encryption [11]-[12]. As we know that embedding gives a more security for the digital data, if the embedding is suspected it may be trivial to retrieve the hidden data. The cover file

will be the container for the given sensitive message. If the cover file itself raises suspicion, it could result in detection of hidden data. A Brazilian drug trafficker had messages hidden with steganographic algorithms hidden on his computer inside images of a cartoon character [7]. Perhaps if the cover image were more innocuous the messages would have escaped detection. While any image can serve as a cover, the images which make the best covers have several properties that make it possible for more of the image's data to be replaced without creating any visually detectable distortion. The most important characteristic of a potential cover is that the image should have a large variety of colors. Images with few colors will make the embedding easier to detect. If, for example, the image is a single color there will be two colors after embedding. These colors will be very similar, but not the same. In Fig. 4, there are two grays that would be produced by a least significant bit embedding. The left side has the gray value 125, and the right 124.

Figure 4. Represents the image with gray 125 left half, gray 124 on right. The difference between the halves may not be detectable.

From the figure 4, we can clearly find out that an image with gray 125 left half and gray 124 on right, this single image is divided into two halves of either equal or un-equal sizes are used for making the cover file un-detectable. An image with many colors is used for embedding the hidden data and the same image after embedding doesn't have much difference and it will not show any difference on the cover medium.

The data file is the file what we want to hide inside the cover file; initially it should be serializable so that it must be embedded bit by bit into the cover file. Normally the data file must be no larger than the cover file, or the cover file would not be able to contain all of the data's information. In our paper we can take cover file of any type like image or audio or video and data file can also be either of image or video or audio so that the size of data file and master file has no constraint. As we are using reversible steganography method ,there is no size limit for master file ,data file as in the reversible steganography we can take input of one file within same type or different file so there shouldn't be any size limitations for both the files. Now let us look at the LSB Insertion technique what we use in this proposed paper.

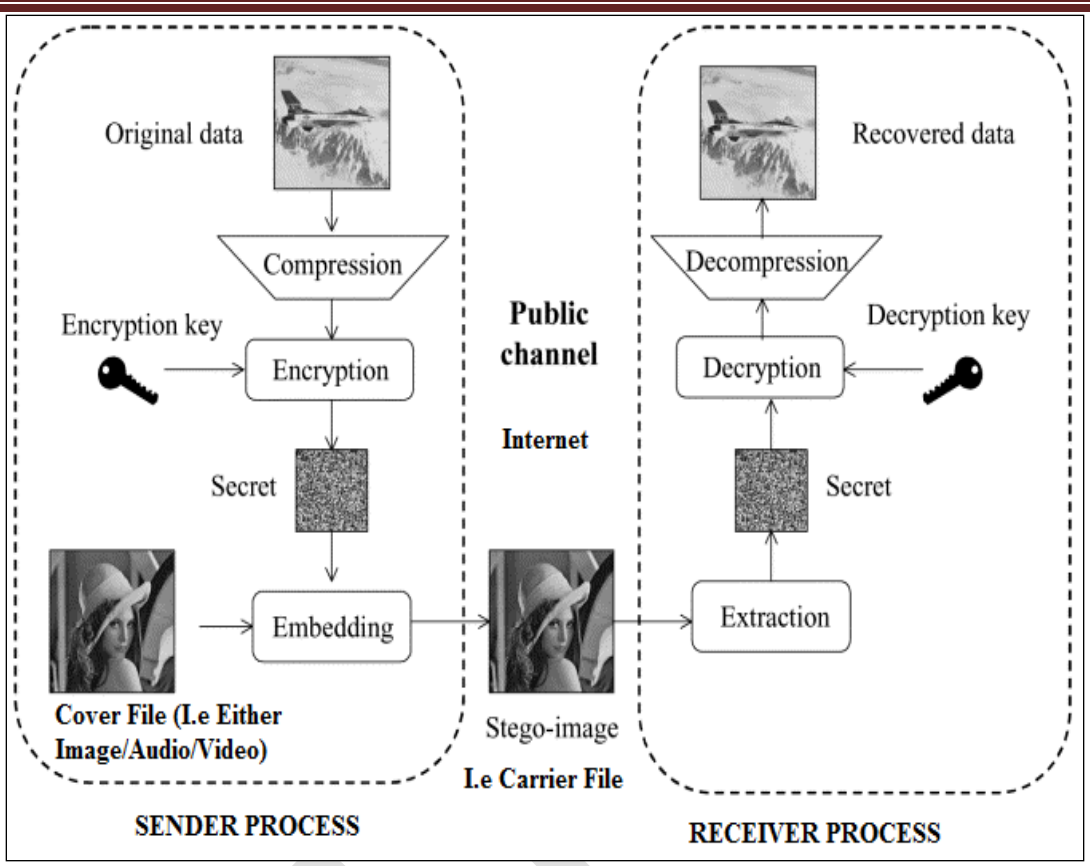


Figure 5 .Represents the Detailed View of Our Proposed Steganography Method

From the figure 5, we can clearly find out the proposed steganography method having two processes, one at sender side and other at receiver side. The sender will initially choose a cover file for storing the sensitive data file inside it, this master or cover file can be either of image, audio or video file. Here the data file can be either of audio, video or image and also text message also (I.e due to because of texture synthesis what we use in our proposed paper).Now the data file is embedded into the cover file and the data is kept secret inside the least significant bits of cover file, we also do encryption for the embedded file as it will give more security for the data from the un-authorized users who try to access the file illegally. During this stage we also do compression of the file as the data file is compressed up to maximum extend so that there will be no loss of any bits from the cover file. Once this is done the resultant file also known as stego-file or carrier file is send to the receiver side, so that the receiver who wish to extract the hidden information need to take the carrier file as input and initially he need to decrypt the data by substituting the valid key that was given by the sender at the embedding side .Once the receiver who satisfies the key value now he can view the data file which is hidden inside the carrier file.

Least Significant Bit (LSB) embedding is one of the best and a simple strategy to implement steganography. Like all the steganographic methods that are available in literature, the LSB algorithm initially embeds the data into the cover or master file and this is saved with a separate new name, so that it cannot be detected by a casual observer. This technique works by

replacing some of the unused parts of the master file with the data that is to be hidden. While it is possible to embed the sensitive or important data into an image/video/audio on any bit-plane, LSB embedding is performed on the least significant bit(s). As the sensitive data what we want to hide is initially converted into bits and these bits will be stored into the master file LSB bits, so that after embedding the bits also it doesn't change its original values. This minimizes the variation in colors that the embedding creates. For example, if we take the embedding example on an image, the embedding into the least significant bit changes the color value by one. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. The steganography method mainly avoids introducing as much variation as possible, to minimize the likelihood of detection. If we directly store the data bits inside an master file LSB area, there is chance of losing some information from the carrier image (I.e. the file which is saved with our own name). This is a major effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide. LSB algorithms have a choice about how they embed that data to hide. They can embed losslessly, preserving all information about the data, or the data may be generalized so that it takes up less space. For getting more efficient result with the LSB algorithm, we are using the compression technique so that some of the bits will be compressed from the cover image and this will reduce the loss of bits from the cover image [8]-[11].

V. CONCLUSION

In this paper, we mainly concentrated on the transmission of sensitive valuable information to different location user with the help of steganography mechanism like hiding valuable data of any type into any type format like audio, video, image.We for the first time have implemented reversible texture synthesis approach for hiding valuable data inside the media files where this process can hide one form of data within same type as well as in different type despite of its size. Initially we target on the problem of hiding sensitive or valuable information into any digital form of data like audio, video, image. As we are using texture synthesis approach in the current paper, we can also hide a valuable text messages in any of the digital data format without affecting the quality or originality of the cover file.

As a future work we want to extend the same steganography concept with double embedding technique, where the double embedding process takes input or master file as either audio or video or image and it will embed any of the formats like audio /video/image as initial hidden file input and it can also take text or message as the second hidden input. So the process of double embedding takes at a time two hidden inputs and save then in a single master file.So that at the receiver end if the receiver enters the correct password ,he can able to extract the two hidden files at a time ,so this gives a better level of security for the data in future.

VI. REFERENCES

[1] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[3] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[4] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.

[5] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*. New York, NY: Plenum, 1984, pp. 51-67.

[6] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.

[7] Three Well Known Authors like Rocha, A., Scheirer, W., & Boult, T. (2011) paper on. Vision of the unseen: Current trends and challenges in digital image and video forensics. *ACM Computing Surveys*. Retrieved from http://dl.acm.org/citation.cfm?id=1978805.

[8] Węgrzyn, M. Virtual Steganographic Laboratory for Digital Images (VSL). Retrieved from http://vsl.sourceforge.net/.

[9] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[10] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "Enhancing the security and quality of LSB based image steganography", 2013 5th International Conference on Computational Intelligence and Communication Networks.

[11] Westfeld, A., & Pfitzmann, A. (n.d.). Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos , and S-Tools — and Some Lessons Learned, 1-16.

[12] *Robert Sugarman (editor) (July 1979). "On foiling computer crime". IEEE Spectrum.IEEE.*

VII .ABOUT THE AUTHORS

SONGA PRATHAP is currently pursuing his 2 Years M.Tech in Computer Science and Systems Engineering,College of Engineering,Andhra University,Visakhapatnam,AP,India. His area of interests includes Network Security.

K.VENKATA RAO is currently working as an Professor, in Computer Science and Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, AP, India. He has more than 15 years of experience in teaching field. His research interest includes Image Processing.