Mixed Stegnography for Providing Security for the Digital Data using LSB Bit-Shifting Algorithm

MADDALA VARALAKSHMI [#1] & D.D.D.SURIBABU [#2] & A.DURGA DEVI [#3],
[#1] M.Sc Student, Master of Computer Science, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#2] Head & Associate Professor, Dept of CSE, D.N.R. College of Engineering, Bhimavaram, AP, India.
[#3] Assistant Professor, Master of Computer Science, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#3] Head & Associate Professor, Dept of CSE, D.N.R. College of Engineering, Bhimavaram, AP, India.

Received: January 12, 2019 Accepted: February 13, 2019

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. Cryptography is the branch of science which try to give utmost security for the text data in terms of encryption and decryption. But this fail to provide security for the digital data(i.e. Image/Audio/Video) in any manner. So in order to provide security for the digital data to transfer from one location to another location in a secure manner, we try to propose a new security primitive like 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. In this proposed thesis we try 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. 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 mixed stegnography gives more security for the digital data in terms of embedding secret data very securely inside the master file compared with the primitive several steganography methods.*

Key Words*: Data Hiding, DES Bit Shifting, Embedding, Encryption, Decryption, Cryptography, Stegnography*

I. Introduction

In this section we will mainly discuss about the preliminary information about the stegnography and its working principle in order to provide data security for the digital data. Now let us look about some of the preliminaries or real time applications where the steganography technique is used.

Steganography on Text Data

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.

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]

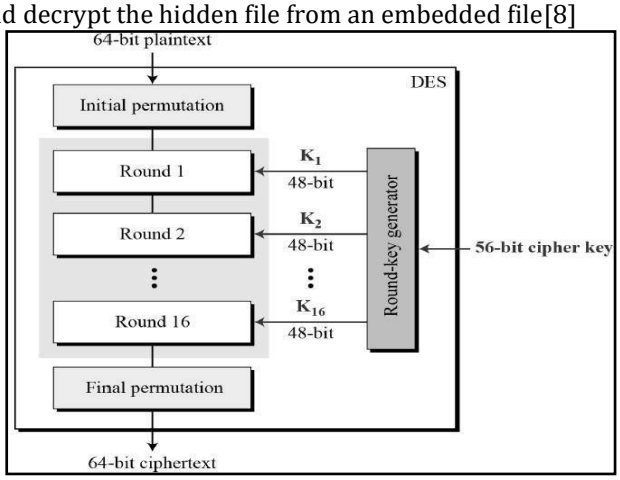


Figure 1. Represents the Architecture of DES Algorithm for Encryption

As we all know that DES algorithm is a symmetric encryption algorithm as shown in above figure 1, 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 [10].

II. Background Knowledge

In this section we mainly try to discuss about the background work that is carried out in order to identify the individual functionalities of each and every module.

Working Principle of Mixed Stegnography

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.

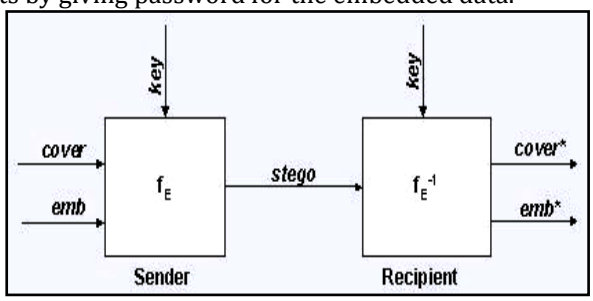


Figure 2. Denote the Working Principle of an Steganographic System

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.

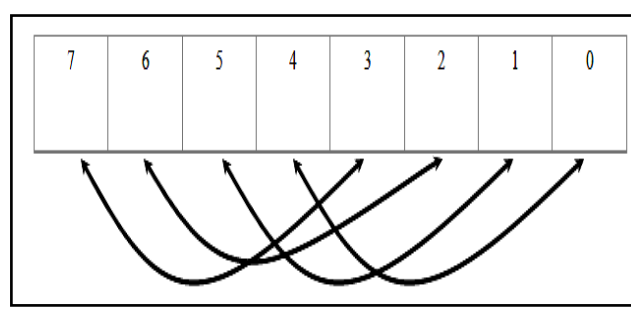
In this current paper, we are not following the primitive cryptographic encryption and primitive cryptographic decryption techniques. We are introducing a novel cryptographic algorithm called as Novel Bit Shift encryption in Random Cycle Order. I.e. totally 4 different types of Bit Shift algorithms are 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[9].

III. Proposed Bit Shift LSB Transformation Approach

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

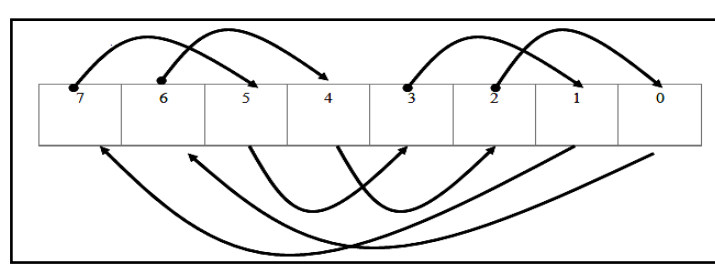
This was the second steganographic technique which was used in order to give more security for the data by applying bit shift operation. There are several types of Bit Shift Operations like 2-Shift, 4-Shift, and 6-Shift and so on. We apply four Bit-Shift operations in the current application in order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

Initial Bit Position



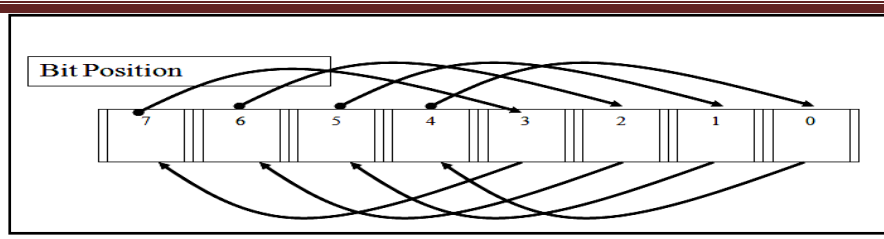
Shift Algorithm – 4 Shift

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.



In this way the bit shifting is used for shifting the data from one bit position to other in the LSB area. So once if the bits are shuffled there is a choice of providing more security for the data.

IV. Conclusion

In this paper we finally implemented a mixed stegnography by using least signification bit shifting approach in order to store one form of data within another form of data either of same data type or different type. Till now there is no single method in the literature of stegnography to hide one form of data within another type of different data types. For the first time we are going to implement this current technique in this current application so that any form of data can be embedded within any format in order to maintain the secrecy of data.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.

V. References

1. 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.
2. Robert Sugarman (editor) (July 1979). "On foiling computer crime". IEEE Spectrum.IEEE.
3. C. Cachin, “An information-theoretic model for steganography,” in Proc. 2nd Intern. Workshop on Information Hiding, Portland, OR, Apr. 1998, pp. 306-318.
4. 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.
5. S. Wang and H. Wang, “Cyber warfare: Steganography vs. steganalysis,” Communications of the ACM, vol. 47, pp. 76-82, Oct. 2004.
6. 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.
7. 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.
8. J. Fridrich, Steganography in Digital Media, Principles, Algorithms, and Applications. Combridge, UK: Combridge Univeristy Press, 2010.
9. 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.
10. Węgrzyn, M. Virtual Steganographic Laboratory for Digital Images (VSL). Retrieved from http://vsl.sourceforge.net/.