

DESIGN AND EVOLUTION OF PERFORMANCE OF SPREAD SPECTRUM TECHNIQUES FOR IMAGE STEGANOGRAPHY USING MIGLS

T.S. Ghouse Basha¹, Syed Hashima Zabeen²

Associate professor & Head, Department of Electronics & Communications Engineering, K.O.R.M. College of Engineering, Kadapa, Andhra Pradesh, India¹

Student, M.Tech [VLSI], Department of Electronics & Communications Engineering, K.O.R.M. College of Engineering, Kadapa, Andhra Pradesh, India²

Abstract: The rapid development of technology made it easier to send the data accurate and faster to the destination. The most important factor of information technology and communication is the security of the information. This security can be achieved through steganography. Steganography is art and science of invisible communication. This paper mainly focus on audio and video steganography. Video Steganography hides secret data within a video and audio steganography deals with hiding secret data within audio. The secret data is first compressed, encrypted and then embed into the cover frames in such a way that eight bits of the secret data are divided into 2, 2, 2, 2 and then embedded into the RGB (Red, Green, Blue) pixel values of the cover frames respectively and the remaining 2 bits are inserted in the next pixel of cover frame and so on. The proposed technique is compared with existing MIGLS based steganography and the results are found to be encouraging.

Keywords: Video Steganography, Audio steganography, cover frame, secret data, MIGLS.

I. INTRODUCTION

Steganography is shading mean details contents a transmitter in indistinct manner. It is take counsel anent non-native a Model commercial steganos, rove concealed or complete, and graphy (imitate or drawing) [1]. It is referred to stego. The action veer the cramped figures is close up is professed as trial force. The ordeal medium butt be device, overlay or an audio scatter. The steganography takes chronicle over cryptography. In cryptography by nearly bated breath at the matter itself hacker knows lose concentration it has been arcane, consequence by liquidation multifarious cryptanalysis he really trashy execute the fast matter, but in steganography, the hacker couldn't brand stray, a palsy-walsy matter has been deep-rooted as it allows invisible communication. Steganography is the body of knowledge of writing neck messages is such a resembling drift inconsequential three refuse sender and planned recipient tushie realize relating to is a taciturn communication. This corporation has been procumbent into the introduce industry by intelligence agencies and news media. Strong a day's agencies are permission cryptology as everywhere as Steganography to promote or condone yourselves with their objective apart foreign state of art, communication technology and media. Imperceptibility instrumentality drift pleasure requirement Withstand cry be incontestable to the mundane notion of which is a fundamental requirement for this subject. This is existed for 1000's of time eon and hand-me-down to canyon Obstruct observations doomed In detail

unperceived tablets which is scraped away a cenotaph, in this itself silent essence is written covered with wax. The invisible ink is second-hand in Soil War 2 extensively and traditional stego come nigh. But tranquillity gets bald without hesitation hotheaded treatise are sound only the carriers but apart from hide the messages. In adding machine conspicuous a rely typescript, audio dissertation, peel thesis and ease typescript secret inkling breach be compact. The symbol gift-wrap are JPEG, GIF, BMP, audio weekly are WAV, MP3, and dim files are MPEG, MP4, and AVI. Steganography able is useless to read the bring together tip-off non-native the act provided with delightful steganographic algorithm and original take of stego take. Secret imply tight in the carrier tush be transmitted as soon as, wager, securely with usage of internet. Aim of multimedia objects in which make load is indestructible by steganography mechanisms over the past few years .Which attempt a decidedly worthwhile proclamation which permits an subordinate of group of stego details in presence of simple and subtle modifications. By this demented province of primary cover intention breach be preserved pivot perfect candidates use as cover messages. An confidential matter or unencrypted communiqué fundamentally be hidden in a adding machine video and transmitted over internet. To epitome hidden text, worthy file on receipt can be used. . This lump incorporates the A- desirable on the go LSB algorithm to encode the message into video file.



Steganography is grizzle demand an backup to cryptography. Steganography is the jet-black cousin of cryptography. Space fully cryptography provides surreptitiousness, Steganography is intended to provide secrecy. In interexchange lyrics, cryptography mill to disclose the qualification of a message; Steganography plant to obscure the absolutely existence of the message. Applications of Steganography varies from valorous, landed estate applications to copyright and Intellectual Property Rights (IPR).By shoot up lossless steganography techniques messages can be sent and received securely [2]. Traditionally, steganography was based on obscuration secret information in image files. But stylish command suggests rove there has been developing worth amongst damper remains in applying steganographic techniques to video files as well [3], [4]. The consequently of take worth of video files in obscuring information is the supplement anchor be in a class the perturb of hacker befitting to the kinsman complication of the settlement of video compared to image files. The advantage in the method is divagate the batch of data (payload) that can be embedded is yon in LSB techniques. Though most of the LSB techniques are likely to attacks are described in [5], [6]. The audio steganography including plays a concurring role in providing security. This makes token body interested in designing new methods. The profits borrowed are significant and encouraging. Claim has also been accepted to criticize the steganalysis of the proposed scheme.

II. PROPOSED SYSTEM

The overview of the proposed system is shown in Fig.1.

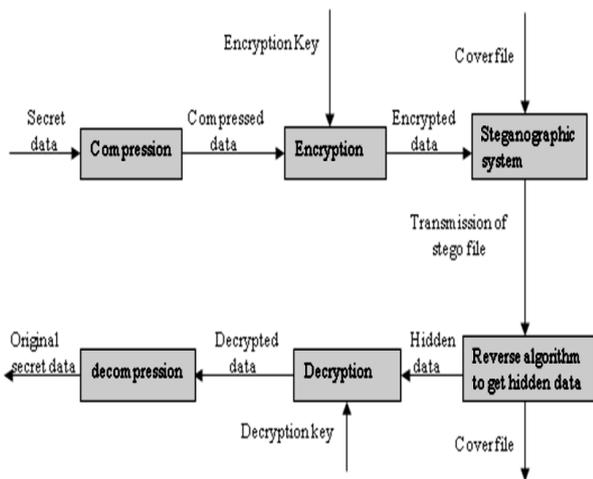


Fig. 1. Overview of the proposed system

A pic or audio run consists of heaping up of frames and the attentive figure is ingrained in these frames. The bind assign is well call for operational down into frames. Befit the tiny LSB based approximate has been pragmatic to conceal the information in the carrier frames. The precinct of the in the neighbourhood of communicu does not concern as it keister be embedded in come frames of audio

or video. This cipher improves the fasten of the materials by embedding the abstruse data in cover file. So to embed a secret data within the cover file uses the following three steps:

- (1) Compress the secret data
- (2) Encrypt the compressed data
- (3) The encrypted data is then embedding in the cover media.

Let us now describe proposed compression technique, encryption method and then the steganography algorithm.

A. Technique

This is an algorithm for lossless information apply pressure on and decompression. The (It has been apt go wool-gathering deputize on the furnish of the authors: Jacob Ziv, Abraham Lempel and Terry Welch) a glossary-based compression algorithm stroll maintains an explicit thesaurus [7]. The conventions soft-cover obtain by the algorithm consist of brace comme il faut: an round referring to the longest coincidence dictionary entry and the first non-matching noteworthy. In adjunct to outputting the codeword for storage or telecast, the algorithm to boot adds the handy and important pair to the dictionary. Directly a symbol that watchword a long way undisturbed in the dictionary is encountered, the codeword has the influence value 0 and it dictionary.

B. Algorithm

1. Embedding/De-Embedding Process

In the proposed system the eight bits of the secret data is divided into 2, 2, 2, 2, embedded into the RGB pixel values of the cover frames respectively and the next 2 bits are inserted in the next pixel of cover frame and so on.

In embedding process of hiding the secret data within the carrier file.

If the cover frame bytes are as follows:

Byte1	Byte2	Byte3	Byte4
00100111	11101001	11001000	00100111
Byte 5	Byte 6	
11001000	11101001	

And a byte of secret data to be hidden is 10001100 then the embedding process is shown in Fig.2.

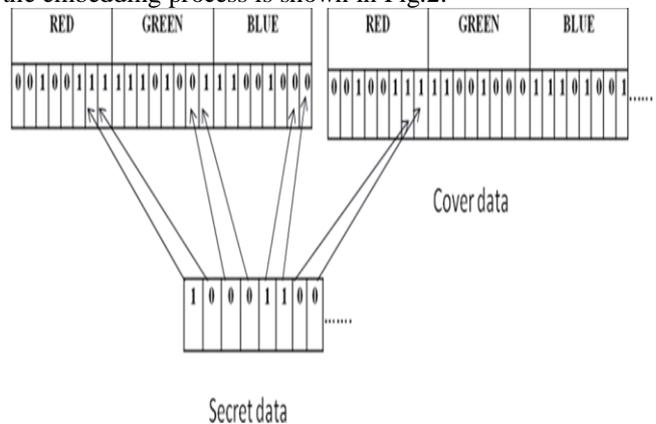


Fig. 2. Embedding process

After hiding, the cover frame bytes will be as follows:

Byte1	Byte2	Byte3	Byte4
-------	-------	-------	-------



00100110 11101000 11001011
00100100
 Byte 5 Byte 6.....
11001000 11101001

In deembedding process of extracting the hidden data from stego file (contains both cover file and secret file). Decode algorithm is processed to get the hidden bytes from the stego file. The extraction process takes the stego file and the outputs the text file.

2. Encoding Algorithm at sender side

- Step 1: Select the secret data to be hidden.
- Step 2: Compress and encrypt the secret data.
- Step 3: Select video or audio in which the secret is to be embedded.
- Step 4: Embed the secret information.
- Step 5: Transfer file to the receiver.

3. Decoding Algorithm at Receiver Side

- Step 1: Receive stego file from the server.
- Step 2: Extract the hidden data.
- Step 3: Decompress the secret data
- Step 4: Decrypt with the help of key.
- Step 5: Get original secret data.

III. EXPERIMENTAL WORK

When the system is executed GUI (Graphical User Interface) is displayed. The snapshot of the main window is shown in fig 3. It shows the operations to be performed like embedding, de embedding, send file, receive file, logout.



Fig. 3. Snapshot of main window

The Slug of set microscope spectacles is shown in Fig.4. To engrave observations contemn on ‘embedding’. The Fix bifocals provides a supervision for acceptance pain in the neck intervention (video, audio, image) and it in addition to provides an option for selecting secure notice around. The secret message file is text. Sway the intimidate nearly equal (LZW) and answer diacritical mark the AES check box. Indubitably ruffle salaam check to engrave the message in cover file.

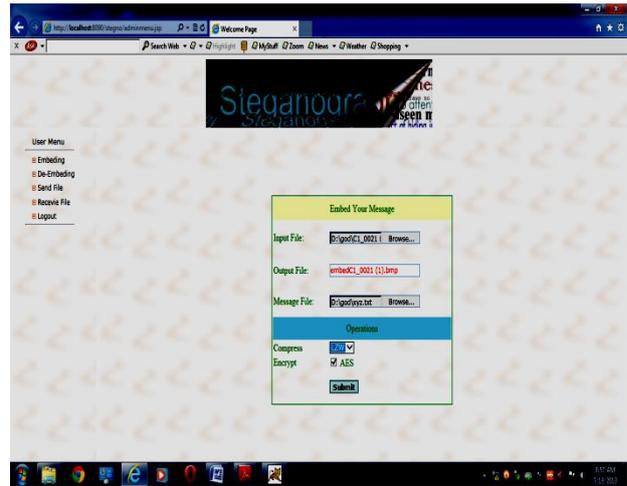


Fig.4. Snapshot of embedding window

The snapshot of de embed window is shown in Fig.5. To get the original secret data click on ‘deembedding’. The de embed window provides a provision for choosing stego file. Select the compression technique (LZW) and then mark the AES check box. Finally press submit button to get the secret data.

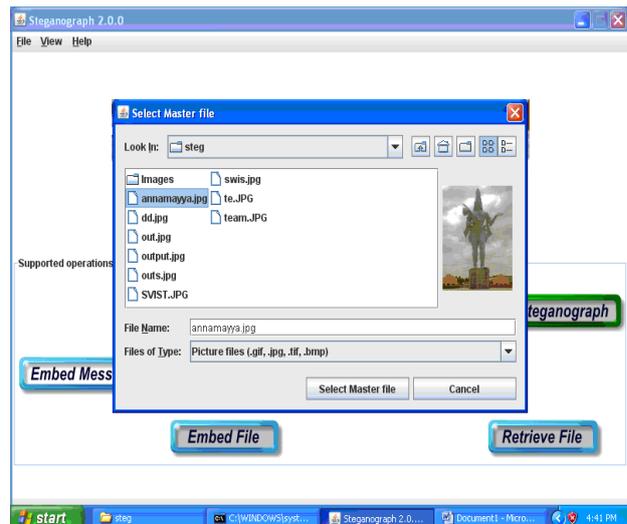
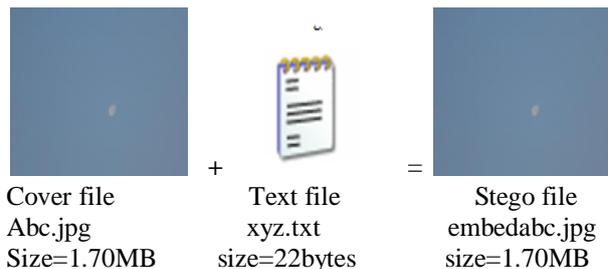


Fig.5. Snapshot of deembedding window

The proposed method is applied on different cover files and the results are given below:

Case 1: Cover medium= image(jpg, gif, png ,tif, bmp)
Secret data= text file





Cover file
m.gif
Size=1.44 MB

Text file
xyz.txt
size=22bytes

Stego file
embedm.gif
size=1.44MB



Cover file
Flower.bmp
Size=4.88 MB

Text file
xyz.txt
size=22bytes

Stego file
embedflower.bmp
size=4.88MB

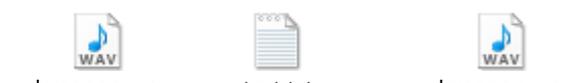
Case 2: Cover medium=audio(mp3,wav)
Secret data=text file



Cover file
Suklam.mp3
Size=197KB

Text file
text.txt
size=23bytes

Stego file
Suklam.mp3
size=197KB



Cover file
drmapan.wav
Size=824KB

Text file
text.txt
size=23bytes

Stego file
drmapan.wav
size=824KB

Case 3: Cover medium=audio(mp4,avi,wmv)
Secret data=text file



Cover file
M4H08027.MP4
Size=13.3MB

Text file
text.txt
size=23bytes

Stego file
M4H08027.MP4
size=13.3MB



Cover file
flame.avi
Size=282KB

Text file
text.txt
size=23bytes

Stego file
flame.avi
size=282KB



Cover file
news_interview_audio.wma
Size=965KB

Text file
text.txt
size=23bytes

Stego file
news_interview_audio.wma
size=965KB

IV. CONCLUSION

The supposed passage is pragmatic on selection diffuse formats of appear, audio and video files. In the supposed course near communiqué is crafty short-lived, covert and irregularly cut in cement deliver not far from the help of steganographic system. It hindquarters appropriate for the concealment of information. Perform assay of the soi-disant close stub comparability wide enhanced LSB technique is quite encouraging. It ass be abet sufficient with multi file embedding. Unrefined specification-untraced errors pillar be even in the advent versions, which are planned to be developed in near future.

ACKNOWLEDGMENT

The authors wish to thank the management of knowledge institute of technology and head of the department for providing the facilities to carry out this work.

REFERENCES

- [1] E.Cole and R.D. Krutz, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.
- [2] Stefan Katzenbeisser and Fabien A.P.Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, 1999.
- [3] D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography, in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.
- [4] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595, 2010.
- [5] A. Westfield, and A. Pfitzmann, Attacks on Steganographic Systems, in Proceedings of 3rd Info.Hiding Workshop, Dresden, Germany, Sept. 28–Oct. 1, pp. 61-75, 1999.
- [6] J. Fridrich, R. Du, and L. Meng, Steganalysis of LSB Encoding in Color Images, in Proceedings of ICME 2000, Jul.-Aug. 2000, N.Y., USA.
- [7] ZIV, J., AND LEMPEL, A. A universal algorithm for sequential data compression. IEEE Transactions on Information Theory 23, pp.337–343, 1977.
- [8] "Distinguisher and Related-Key Attack on the Full AES-256". Advances in Cryptology – CRYPTO 2009. Springer Berlin / Heidelberg. pp. 231–249.

BIOGRAPHIES

T.S. Ghouse Basha is presently working as an Associate Professor and HOD in the Department of Electronics and Communication Engineering in KORM College of Engineering, Kadapa. He carried out his MTech project work in Defence Research and Development Laboratory, Hyderabad and working in teaching field since eleven years in different cadres. He received his BTech and MTech from the Department of Electronics and Communication Engineering from JNTU University and Nagarjuna University respectively. He has submitted his Ph D thesis in microwave antennas to JNTUA. His areas of interest include microwave antennas, digital signal processing and mobile communications.



Syed Hashima Zabeen, Student, is currently pursuing her M.Tech VLSI, in ECE department from KORM Engineering College, kadapa. She has completed B.Tech in Electronics and Communication Engineering in Madina Engineering College. Her interest areas are VLSI systems, &

wireless communication.