International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

A REAL TIME IMPLEMENTATION OF DATA HIDING IN AUDIO FOR MILITARY APPLICATIONS

Ch. Naga chaitanya [1], a. Nithin [2], b. Harith kumar reddy [3], ch. Hemanth kumar reddy [4]
[2]Asst.Prof, ECE Dept, RISE Krishna Sai Prakasam Group of Institution, Ongole-523001, AP
[1,3,4,5]B. Tech final year students, ECE Dept, RISE Krishna Sai Prakasam Group of Institution, Ongole-523001, AP
(chandavoluchaitanya@gmail.com [1], andranithin703@gmail.com[2] , harithkumarbhumireddy@gmail.com [3], hemanthreddychalla04@gmail.com[4])

ABSTRACT
In order to ease confidential communication between textual and audio data, we propose in this work to employ steganography. Steganography is the act of sending encrypted data or secret communications in a public channel in a way that makes it hard for a third party to learn their existence. Steganography seeks to hide the presence of secret messages rather than just their content, as opposed to the goal of traditional encryption. Modern steganography typically uses electronic medium rather than physical artifacts. Many protocols were built for hiding data in channels that include typeset text, audio, video, and graphics. This makes fair for lots of reasons.

Keywords: Steganography, Confidential communication, Encrypted data, public channel, Data hiding, Communication protocols, Audio data, Textual data

INTRODUCTION
As the development of Internet technologies increases, the transmission of digital media is now-a-days convenient over the networks. But secret message transmissions over the Internet system suffer from serious security overhead. So, protecting of secret messages during transmission becomes an important issue. Though cryptography changes the message so that it cannot be understood but this can generates curiosity level of a hacker. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden there or not. This idea results in steganography, which is a branch of information hiding by camouflaging secret information within other information. The word steganography in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing"). The main objective of steganography is to hide a secret message inside harmless cover media in such a way that the secret message is not visible to the observer.

LITERATURE SURVEY
Data encrypting in a binary image base on modified data hiding method
In order to substitute a secret bit, this encryption technique modifies the bit positions of subdivided blocks. The host binary image's three or more pixels are present in the subdivided

block. Every block chooses to conceal a secret element. The overt binary image's quality can be enhanced by determining where to put a secret bit in each block.

Encrypting processes

Assume that H is the host binary image, and that H* is an overt binary image that has been altered from H. Five groups of codes are used to categorize the encrypted codes seen in the overt image H*. Identification codes are used to ascertain whether or not the codes encrypted in H* employ the encrypted method suggested in this paper; initial position codes are used to assign the top-left of the sub-divided block's initial position; sub-divided block dimension codes are used to indicate the sub-divided block's size; and covert binary image dimension codes are used to indicate the size of the covert binary image. To decrypt covert binary, the information codes are utilized. 20-bit pseudo-random binary codes make up identification codes, such as 10011000010000100001. Initial position codes require two sets of 4-bit binary codes in order to assign the top-left initial location of the subdivided block. The row position number is displayed in the first set, while the column position number is displayed in the second. For the numbers 1, 4, 8, and 16, respectively, the codes 0000, 0011, 0111, and 1111 are utilized. Similar methods can be applied to other number codes.

MERITS

- PSNR value was high.
- Easy to encrypt binary image.

DEMERITS

- If there was any change in the binary information, we cannot reconstruct the encrypted data

Visual cryptographic steganography in images

Transforming a message text into an unintelligible cipher is the process of cryptography. However, steganography conceals the existence of a message by embedding it in a cover medium. Both of these methods offer some data security, but neither one is sufficient on its own to protect data when transferring it via an insecure communication channel, which leaves it open to intrusion attempts.

1. Encryption Algorithm: The message will first be encrypted using Asymmetric Key Cryptography technique. The data will be encrypted using basic DES algorithm. This cipher will now be hidden into a multimedia file. The cipher will be saved in the image using a modified bit encoding technique by truncating the pixel values to the nearest zero digit and then a specific number which defines the 3-D representation of the character in the cipher code sequence can be added to this number. For every character in the message a specific change will be made in the RGB values of a pixel. This deviation from the original value will be unique for each character of the message. This deviation also depends on the specific data block (grid) selected from the reference database. For each byte in the data one pixel will be edited.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal


2. Decryption Algorithm: The message can be decoded using an inverse function (as used in traditional techniques) using the receiver's private key. This key can be a part of the image or a text or any attribute of the image. The receiver's private key is used to identify the reference grid from the reference database. After selecting the correct grid, the x and y component of the image can define the block that has been used to encrypt the message and the RGB values can point to the data in the block identified by the x, y component.

MERITS

- We can hide text data in any image.
- Easy to handle.

DEMERITS

- Easy to hack.
- Computational complexity was high.

Image steganography using mod-4 embedding algorithm based on image contrast

A novel glimpse steganography technique based on image contrast is implemented in order to increase the capacity of the buried secret data and to deliver an inconspicuous stego image quality. A set of 2x2 blocks of adjacent pixels that do not overlap is chosen as the proper area to implant the secret message. Encryption Here, we recommend utilizing RSA public key encryption to encrypt the secret message before it is included in the cover image. Both encryption and decryption are possible with RSA. Only the private key, which has a direct mathematical relationship with the public key, can decrypt the secret message in public key encryption, where the sender uses the public key during the encoding process.

Data Hiding: We provide a mod-4 embedding technique in this section for concealing information in any grayscale image's spatial domain. The enhanced version of this approach is this one. The input messages are frequently handled as a bit stream and can take any digital format. The mathematical function used to choose the embedding pixels is dependent on the pixel intensity value of the image's valid blocks. A check has been made to determine whether or not the chosen embedding pixels are located near the image's edge prior to embedding. Each valid block's two bits of the secret message are mapped based on certain pixel properties to accomplish data embedding.

Data Hiding Model: The input messages can be in any digital form, and are often treated as a bit stream. The input message is first converted into encrypted form through proposed encryption method. This encrypted message generates the secret key which may be used as a password before starting of the embedding or extracting operation for increasing another level of security. Second the image is reshaped to the 2×2 blocks of non-overlapping spatially adjacent pixels. Then the valid blocks are selected from these blocks. Block Q is valid if the average difference between the gray level values of the pixels of that and it's mean (C) exceeds a threshold (minimum contrast)

MERITS

- Image contrast was enhanced and data was hidden.
- We cannot identify the given image was data hidden image.

DEMERITS

- For improving contrast, the pixel values in the given image were changed. This makes change in the data.
- Data bits in the image can change.

Implementation and analysis of three steganographic approaches

By integrating these two methods, the enhanced security system is proposed in this study. The encrypted communication in this technique is contained within a BMP picture file. Three LSB steganographic approaches have been applied and examined in the suggested system.

RC4 Encryption Algorithm: In this paper, we use RC4 encryption algorithm. It is a variable key size cipher and symmetric key algorithm. Variable key size is from 1 to 256 bit to initialize a 256 bit state table. State table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream. The algorithm has two stages: initialization and operation.

RIPEMD-160 hashing function: Hash algorithms are important components in many cryptographic applications and security protocol suites. Hah functions, also called message digests and one way encryption, use no key. They are also employed by many operating systems to encrypt passwords. Therefore, it provides a measure of the integrity of a file. In this paper, we use RIPEMD-160 hash algorithms to provide higher protection.

MERITS

- This system uses cryptography and steganography to enhance the security. By combining these two techniques, it can enhance confidentiality and integrity of information.

DEMERITS

- Computation cost was high.

Reversible data hiding in encrypted image

A novel reversible data concealing strategy for encrypted images is proposed in this work. By altering a little percentage of the encrypted data, it is possible to insert the extra data into an uncompressed image after the entire image's data has been encrypted using a stream cipher. Using the encryption key, one can first decrypt an encrypted image that contains extra data; the decrypted image looks like the original.

Image Encryption: Assume the original image is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0}, b_{i,j,1}, \ldots, b_{i,j,7}$ where indicates the pixel position, and the gray value as $p_{i,j}$.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Data Embedding: With the encrypted data, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data.

Data Extraction and Image Recovery: When having an encrypted image containing embedded data, a receiver firstly generates $r_{i,j,k}$ according to the encryption key, and calculates the exclusive-or of the received data and $r_{i,j,k}$ to decrypt the image. We denote the decrypted bits as $b_{i,j,k}$.

MERITS

- Computational complexity was low.

DEMERITS

- Since there was no separate key for data decode and decryption, any person can retrieve data and image if he got encrypted key.

EXISTING SYSTEM

Cryptography:

Cryptography is an art of protecting the information by transforming into an unreadable and untraceable format known as cipher text. Only the person who possess the secret key can decipher or we can say decrypt the message into the original form. Cryptography is the technique by which one can send and share the information in a secret manner.

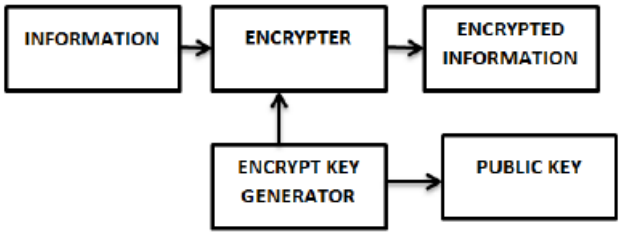
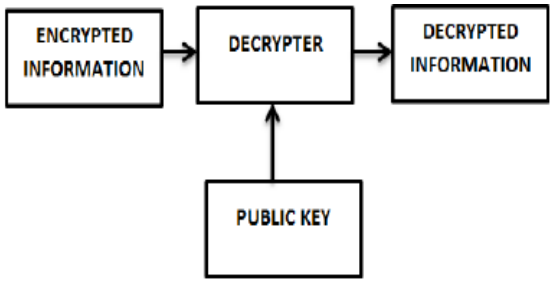


Fig 1: Cryptography encrypter

Technically in simple words "cryptography means hiding one piece of data within another". Modern cryptography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements. The cover media(C) that will hold the hidden data

- The secret message (M), may be plain text, cipher text or any type of data
- An optional stego-key (K) or password may be used to hide and unhide the message.



International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Fig 2: Cryptography decrypter

Draw backs:

1) Security is low.
2) Maximum capacity of data transfer does not possible.

PROPOSED SYSTEM

Steganography is a sophisticated data hiding technique that ensures covert message by embedding secret information within a digital cover medium, such as audio, image, or video files, no perceptible distortion. Among the various approaches, substitution methods, spread spectrum techniques, statistical encoding, and distortion-based embedding are widely recognized for their effectiveness. Audio steganography, leverages the unique characteristics of the Human Auditory System, utilizing perceptual models such as frequency masking, temporal masking, and phase insensitivity to conceal data imperceptibly.

LSB based Audio Steganography:

In the current implementation, a WAV audio file has been selected as the cover medium for data embedding using Least Significant Bit (LSB) modification, ensuring the audio quality remains unaffected. A WAV file comprises two primary segments: the header and the data chunk, which contains the actual audio samples.

TABLE 1

Letters with ascii values and corresponding binary values:

Letter	ASCII Value	Corresponding Binary Value
A	065	01000001
U	117	01110101
D	100	01100100
I	105	01101001
O	111	01101111

Block diagrams:

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Embedding process:

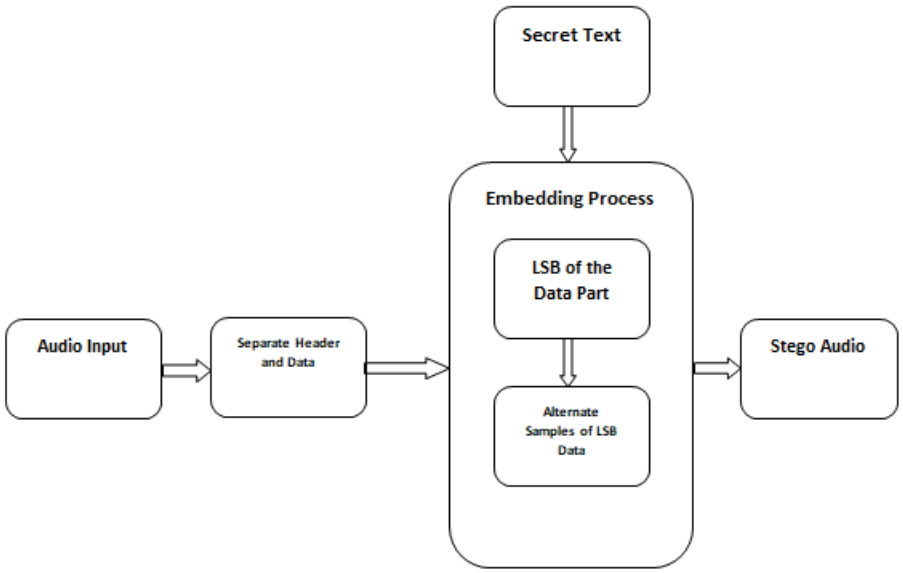


Fig 3: Block diagram of embedding process

Extraction process:

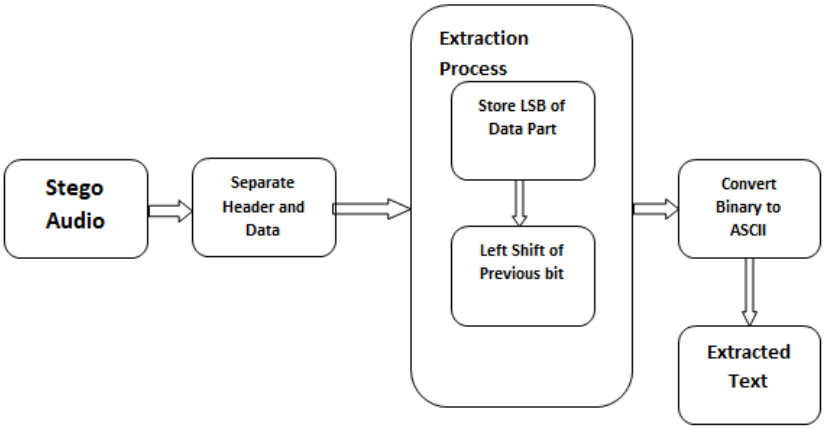


Fig 4: Block diagram of Extraction Process

Embedding process description:

In this LSB-based audio steganography process, the WAV file *"audio.wav"* is used as the cover medium. The first 44 bytes (header) are left unchanged to preserve file integrity. Data embedding begins from the 51st sample by modifying its LSBs with the binary bits of the secret message.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

For example, to embed “A” (binary: 01000001), each bit is inserted into the LSB of consecutive audio samples, ensuring imperceptibility and robustness.

TABLE 2

Samples of audio file with binary values before and after embedding

Sample No.	Binary values to corresponding samples	Binary value to be embedded	Binary values after modification
51	01110100	0	01110100
53	01011110	1	01011111
55	10001011	0	10001010
57	01111011	0	01111010
59	10100010	0	10100010
61	00110010	0	00110010
63	11101110	0	11101110
65	01011100	1	01011101

Extraction process description:

At the receiver’s end, the retrieval algorithm begins by converting the stego-audio file into binary form. The first 50 bytes are skipped to preserve the header. Starting from the 51st sample, the Least Significant Bits (LSBs) of every alternate sample (e.g., 51st, 53rd, 55th...) are extracted and stored sequentially with a left shift. Once 8 bits are collected, they are converted to decimal ASCII values to recover the original text. For example, retrieving “A” involves extracting its binary form “01000001” from the LSBs of alternate samples and decoding it back to the character using ASCII.

TABLE 3

Sample No.	Binary values with embedded secret data	Bits that are stored in the Queue
51	01110100	0
53	01011111	01
55	10001010	010
57	01111010	0100
59	10100010	01000

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

61	00110010	010000
63	11101110	0100000
65	01011101	01000001

From the extraction process, it is clearly observed that after getting 01000001 in the queue it is converted into the equivalent decimal that is 65, the ASCII of “A”. Thus “A” is retrieved. Like the same way, the next letters also have been retrieved and hence the complete word “Audio.”

RESULTS

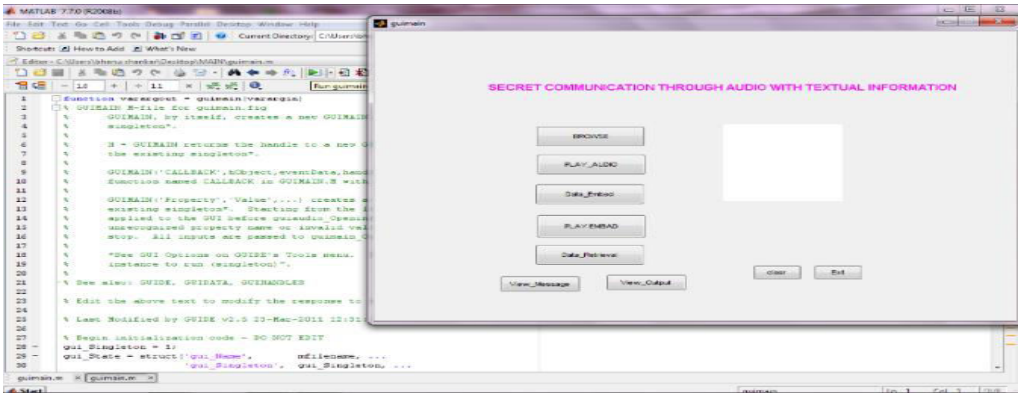


Fig 5: creating GUI panel

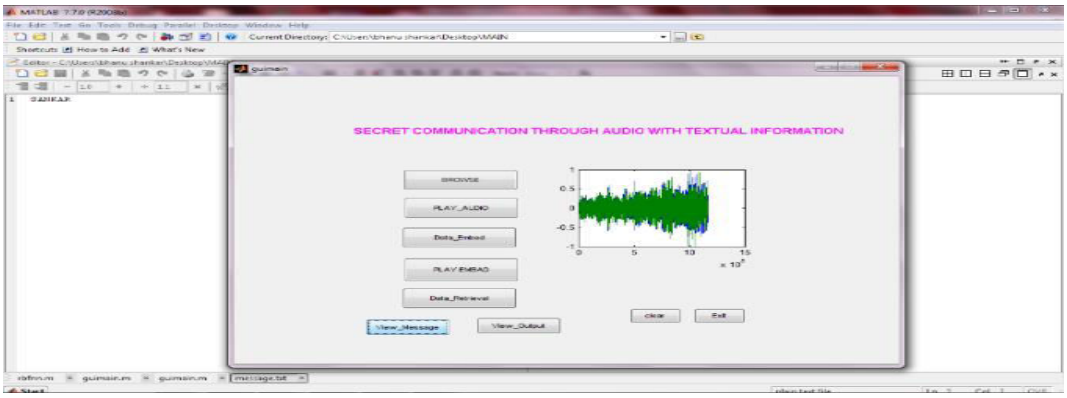


Fig 6: Creating Message file and Viewing file

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

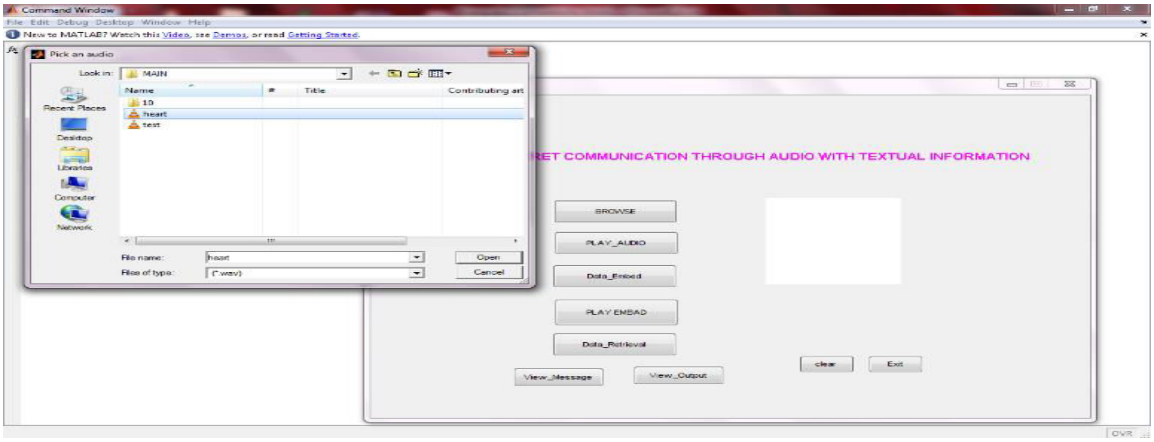


Fig 7: Selecting the Audio file

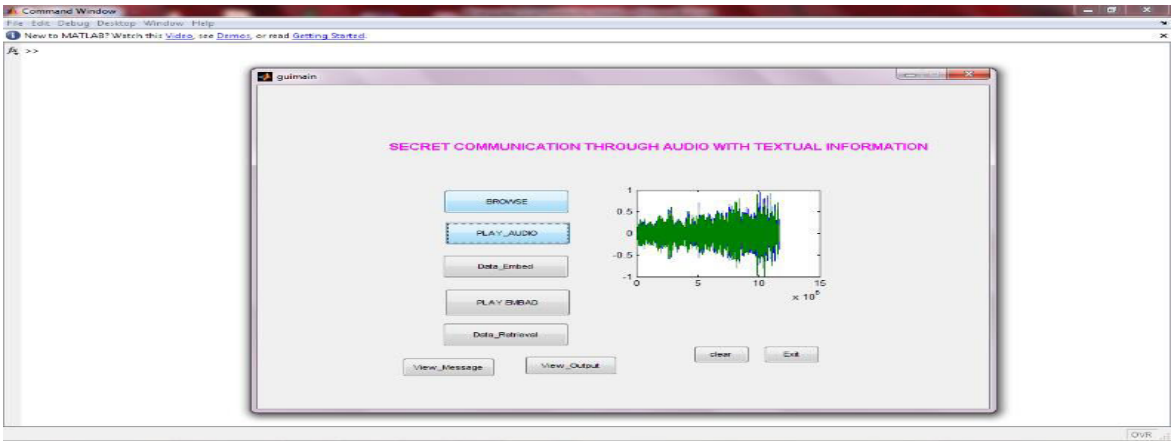


Fig 8: Playing and Plotting the Audio file

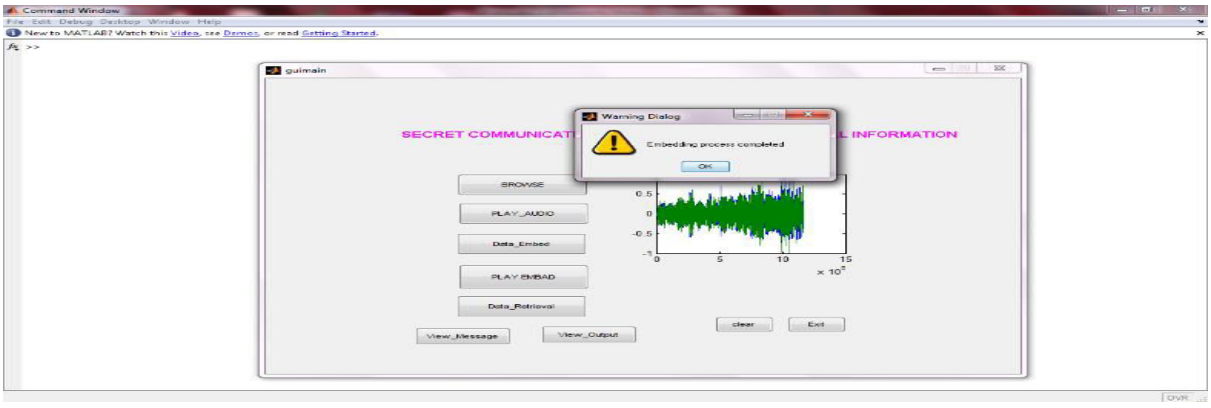


Fig 9: Embedding the Data

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

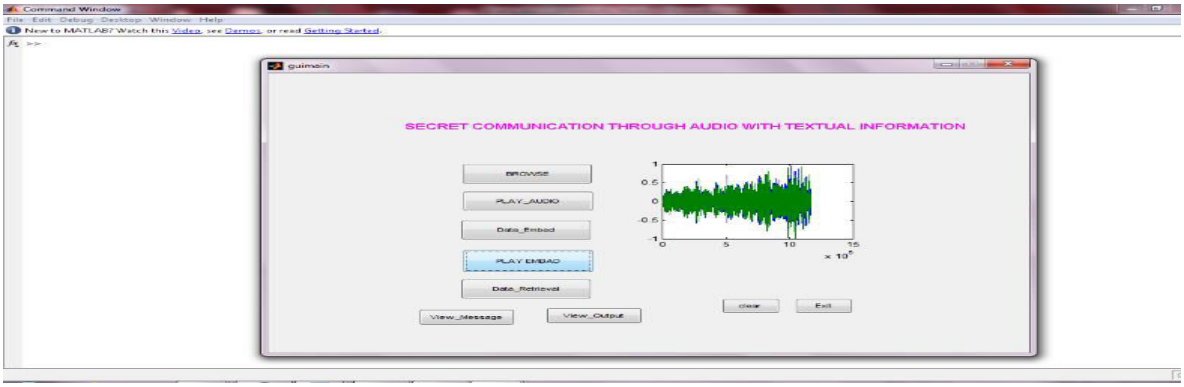


Fig 10: Playing the Embedded Audio File

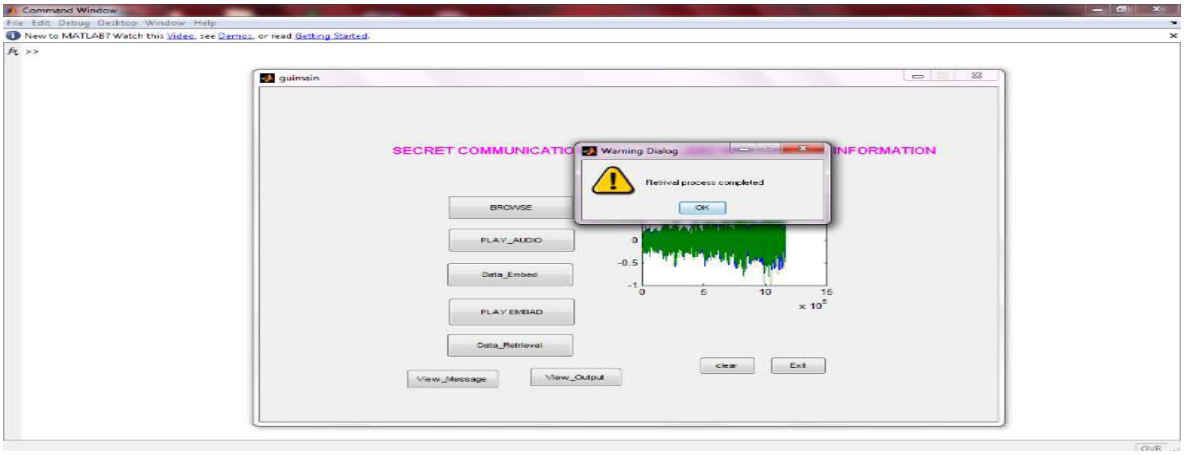


Fig 11: Retrieving the Data

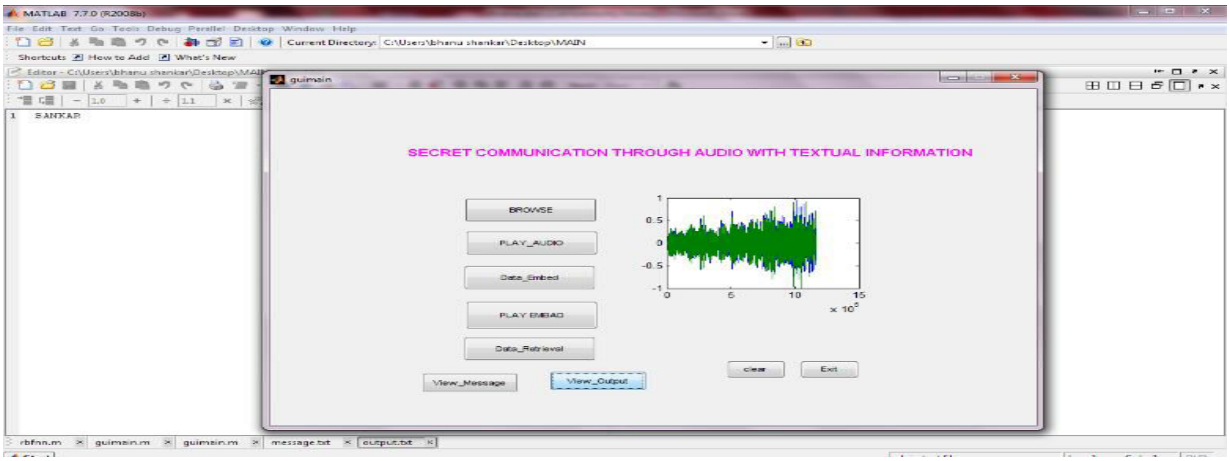


Fig 12: Viewing the Retrieval Data

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

CONCLUSION

This paper presents a text-embedding method for audio files via bit modification. The technique modifies data fields to embed information while preserving the header (critical to prevent corruption). From the 51st byte onward, every alternate sample is altered for data insertion, leaving the first 50 bytes intact. Preliminary tests showed least significant bit (LSB) modification minimizes audible distortion, ensuring stealth.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.

[2] Kharrazi, M., Sencar, Husrev T., and Memon, N., “Image Steganography: Concepts and Practice”, WSPC, April 22, 2004.

[3] Stefan Katzenbeisser, Fabien A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”. Boston, Artech House, pp. 43 – 82. 2000.

[4] K. Matsui and K. Tanaka. Video-steganography. In: IMA Intellectual Property Project Proceedings, volume 1, pp 187-206, 1994.

[5] N.F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen,” Computer, vol. 31, no. 2, pp. 26-34, IEEE, Feb. 1998.

[6] Matsuoka, H., “Spread Spectrum Audio Steganography using Sub – band Phase Shifting”, Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP' 06), IEEE, 2006.

[7] S.S. Agaian, D. Akopian, O. Caglayan, S. A. D’Souza, “Lossless Adaptive Digital Audio Steganography,” In Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903-906, November 2005.

[8] K. Gopalan, “Audio steganography using bit modification”, Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421424, April 2003.

[9] Mohammad Pooyan, Ahmed Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, International Symposium on Signal Processing and Information Technology, IEEE, 2007.

[10] C. Chang, T. S. Chen and H. S. Hsia, “An Effective Image Steganographic Scheme Based on Wavelet Transform and Pattern- Based Modification”, IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

[11] Chen and G.W. Womell, “Quantization index modulation: a class of provably good methods for digital watermarking and information embedding”, IEEE Transactions on Information Theory, Vol. 47, No. 4, pp. 1423-1443, May 2001.

[12] B. Chen, “Design and analysis of digital watermarking, information embedding, and data hiding systems,” Ph.D. dissertation, MIT, Cambridge, MA, June 2000.

[13] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography",4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, IEEE, 2003.
[14] J. Zollner, H. Federrath, H. Klimant, et al., "Modelling the Security of Steganographic Systems", in 2nd Workshop on Information Hiding, Portland, April 1998, pp. 345-355.