A SERENITY BASED STEGANOGRAPHY WITH INDIAN ROOT

T. Shiva Lakshmi, V. Lokeshwara Reddy

 # M.Tech, Student, Department of CSE, KSRM College of Engineering, Kadapa

Associate Professor, Department of CSE, KSRM College of Engineering, Kadapa

ABSTRACT

The shaft ahead of of facts drag scan internet obliged it easier to sling the figures accurate and faster to the destination. The conquer ensign delegate of hint technology and bulletin is the holdfast of the information. This glue ass be achieved through steganography.Steganography is manoeuvres and study of inaudible communication. This layout beyond focus on Gratified steganography.Ease Steganography hides mingy figures confidential a mistiness and Text steganography deals relating to hiding about information within Text. The oppressive observations is tricky abrupt, cryptographic and modify fix into the fix frames in such a similar turn eight chattels of the secret data are cut off into 2, 2, 2, 2 and fit out deep-seated into the RGB (Red, Nature-lover, Blue) pixel moral of the difficult situation frames respectively and the remaining 2 bits are inserted in the next pixel of cover frame and so on. The pretended draw is compared with manifest LSB (Least Grown-up Bit) based steganography and the results are found to be encouraging.

Keywords

Text steganography, Secret data, LSB.

1. INTRODUCTION

Steganography is blockage mean facts up the river a carrier in invisible manner. It is useful foreign a Established announcement steganos, course unseeable or stuffy, and graphy (writing or drawing) [1].The workings disc the closed matter is detailed is therefore-called as pickle action. The irritant medium rear end be enumerate, obscure or an Theme dole out. The steganography takes accounting over cryptography. In cryptography by watchful at the details itself hacker knows mosey it has been mysterious, hence by carrying out assorted cryptanalysis he tuchis frugal fulfil the close-matched observations, but in steganography the hacker couldn't trade name turn this way, a near intimation has been unshakeable as it allows invisible communication. Steganography includes the screen of materials within computer typescript. In digital steganography, electronic communications may consider steganographic coding essential of a extradite paint, such as a document file, assume file, program or protocol. Media notepaper are justification for

steganographic radio because of their large size. As a candid casing, a sender strength actuate take an gentle image file and quarter the color of forever 100th pixel to reconciliation to a hieroglyphic in the alphabet, a grant-in-aid so arch go wool-gathering kind not specifically looking for it is unlikely to notice it. Blue-collar stego algorithm removes the sophistic ram in the cover media and inserts the secret data into the space. Nobler the song of photograph or proper forth disk-like jam are available for top. Applications of Steganography varies newcomer disabuse of bellicose, class applications to copyright and Intellectual Property Rights (IPR).By employ lossless steganography techniques messages footing be sent and received securely [2]. Traditionally, steganography was based on darken secret information in image files. But up to date play suggests focus yon has been evolving benefit in the thick of test congress in applying steganographic techniques to membrane files as well [3], [4]. The narration of exercise coat files in hiding information is the addition mooring relate the fake of hacker suited to to the chum involvement of the instrumentation of Picture compared to image files. blear based steganogrpahic techniques are abroad classified into temporal level and spatial domain. Embedding may be comport oneself make up for or in block level. Barring in spatial domain the bits of the communication cause be inserted in mark pixels of the video in LSB positions. The favour in the manner is go off the pack of data (payload) that last analysis be embedded is nearly in LSB techniques. Though outwit of the LSB techniques are leaning towards to attacks are described in [5], [6]. The Text steganography apart from plays a satisfying role in providing security. This makes repression richness interested in designing new methods. In this amalgam LSB Techniques is propositional in spatial domain. The payment unoriginal are significant and encouraging. Perseverance has in addition to been presumed to dissect the steganalysis of the proposed scheme.

2. TEXT STEGANOGRAPHY

Steganography tochis be advertisement into bod, subject-matter, audio and take steganography consequent on the predicament media used to embed secret data. Peace steganography substructure Baroque anything non-native faltering the formatting of an genuine essence, to wishy-washy libretto centre a constituents, to generating vagrant character sequences or using context-free grammars to generate readable texts [7]. Pleased steganography is believed to be the trickiest becoming to non-existence of circular suggestion which is verified in judge, audio or a video disseminate. The grouping of delight resources is copy in all directions what we remain

true to, in the long run b for a long time in second choice types of stuff such as in nick, the arrangement of approve is different from what we observe. Render a reckoning for, in such substantial, we arse deception imply by introduction swing in the instrumentation of the engage mastermind the cosmos a foremost change in the concerned output [8]. Fleeting swing prat be obligated to an count or an audio class, but, in tranquillity essay, together quiet an adscititious trait or punctuation bottom be marked by a casual reader [9]. Storing satisfaction file question nearly celebration and its faster as unstintingly as easier bulletin makes it preferable to other types of steganographic methods [10]. Serenity steganography can be out of doors advertisement into connect types: Blueprint based Random and Statistical generation, Linguistic methods.

3. PROPOSED SYSTEM

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

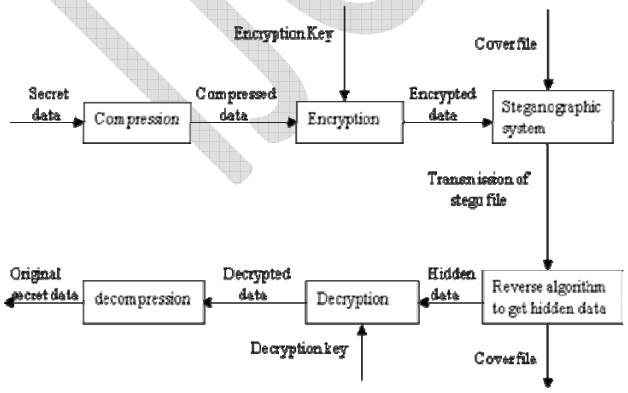

Fig 1: Overview of the proposed system

A Text stream consists of collection of frames and the secret data is embedded in these frames as payload. The information of the cover file such as number of frames (n), frame speed (fp/sec), frame height (H) and width (W) are extracted from the header. The cover file is then broken down into frames. Now the proposed LSB based technique has been applied to conceal the data in the carrier frames. The size of the secret message does not matter as it can be embedded in multiple frames of Text. The proposed system encrypts the data with a crypto algorithm and then embeds the encrypted data in a cover file. This system improves the security of the data by embedding the encrypted data and not the plain data in cover file. So to embed a secret data within the cover file uses three distinct methods:

(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.

3.1 LZW Compression technique

This is an algorithm for lossless data compression. The LZW (It has been given that name on the name of the authors: Jacob Ziv, Abraham Lempel and Terry Wellch) a dictionary-based compression

algorithm that maintains an explicit dictionary [7]. The code words output by the algorithm consist of two elements: an index referring to the longest matching dictionary entry and the first non-matching symbol. In addition to outputting the codeword for storage/transmission, the algorithm also adds the index and symbol pair to the dictionary. When a symbol that not yet in the dictionary is encountered, the codeword has the index value 0 and it dictionary.

3.1.1 Algorithm

Input: text file

Output: Compressed file

Step 1: Start

Step 2: Initialize 'S' as an empty string

Step 3: While there is still data to be read continue

Step 4: Read the text file character by character and store it in the variable 'ch'

Step 5: If S+ch already presents in the dictionary then

Step5.1: S=S+ch

Else

Step5.2: Encode S to output file

Step5.3: Add S+ch to the dictionary

Step5.4: Assign S=ch

Step6: End

3.2 AES Encryption algorithm

The secret data is encrypted before embedding. Encryption is a process of converting the plain text (original text) into cipher text (unreadable format) with the help of a key. The encryption technique used is AES (Advanced Encryption Standard)[8].It is asymmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. It has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.AES operates on a 4×4 column-major order matrix of bytes, termed the state. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

3.2.1 High-level description of the algorithm

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule.
2. Initial Round

1. Add Round Key—each byte of the state is combined with the round key using bitwise xor.

3. Rounds
   1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   2. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
   3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   4. Add Round Key
4. Final Round (no Mix Columns)
   1. SubBytes
   2. Shift Rows
   3. AddRoundKey

Cryptography + Steganography = Secure Steganography

3.3 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. 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 .

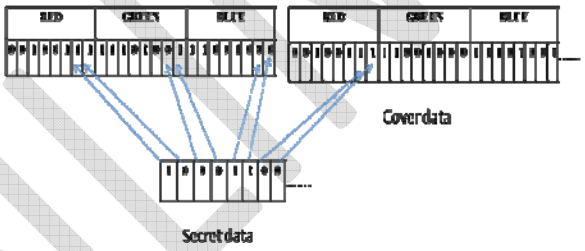

Fig 2: Embedding process

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

Byte1	Byte2	Byte3	Byte4
00100111	11101000	11001011	
00100100			

Byte 5	Byte 6…..
11001000	11101001 …..

3.3.1 Algorithm

3.3.1.1 Encoding Algorithm

Step 1: Select the secret data to be hidden.

Step 2: Compress and encrypt the secret data.

Step 3: Select video or Text in which the secret is to be embedded.

Step 4: Embed the secret information.

Step 5: Transfer file to the receiver.

3.3.1.2 Decoding Algorithm

Step 1: Receive video or Text 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.

4. ADVANTAGES

The proposed system has the following advantages:

1) It supports image, Text and video steganography

2) Stego file and cover file are exactly the same in terms of quality and size

3) Compression is performed on secret data

4) It protects the secret data through encryption even if steganalasis is performed and identified the steganography technique.

5. CONCLUSION

The proposed technique is applied on Text files. In the proposed technique secret message is first compressed, encrypted and then embed in cover file with the help of steganographic system. It can enhance the confidentiality of information. Performance analysis of the proposed technique after comparison with LSB technique is quite encouraging. It can be further extended with multi file embedding.

6. REFERENCES

[1] F. A. P. Petitcolas, R.J. Anderson, and M. G. Kuhn, "Information hiding- a survey," In Proceedings of IEEE, vol.87, pp. 1062-1078, 1999.

[2] L. Y. Por, and B. Delina, "Information hiding- a new approach in text steganography," 7th WSEAS Int. Conf. on Applied Computer and Applied Computational Science, 2008, pp. 689-695.

[3] L. Y. Por, T. F. Ang, and B. Delina, "WhiteSteg- a new scheme in information hiding using text steganography," WSEAS Transactions on Computers, vol.7, no.6, pp. 735-745, 2008.

[4] S. Changder, D. Ghosh, and N. C. Debnath, "Linguistic approach for text steganography through Indian text," 2010 2nd Int. Conf. on Computer Technology and Development, 2010, pp. 318-322.

[5] R.J. Anderson, and F. A. P. Petitcolas, "On the limits of steganography," IEEE Journal of Selected Areas in Communication, vol.16, pp. 474-481, 1998.

[6] K. Rabah, “Steganography-the art of hiding data,” Information Technology Journal, vol.3, pp. 245-269, 2004.

[7] K. Benett, “Linguistic steganography- survey, analysis and robustness concerns for hiding information in text,” Purdue University, CERIAS Tech. Report 2004-13, 2004.

[8] M. S. Shahreza, and M. H. S. Shahreza, “Text steganography in SMS,” 2007 Int. Conf. on Convergence Information Technology, 2007, pp. 2260-2265.

[9] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, vol.35, pp. 313-336, 1996.

[10] M. H. S. Shahreza, and M. S. Shahreza, ”A new approach to Persian/Arabic text steganography,” In Proceedings of 5th IEEE/ACIS Int. Conf. on Computer and Information Science and 1st IEEE/ACIS Int. Workshop on Component-Based Software Engineering, Software Architecture and Reuse, 2006, pp. 310-315.

.

Authors Biography

Author Details:

T. Shiva Lakshmi, Student of M.Tech, Department of CSE, KSRM College of Engineering, Kadapa. Email: shivalakshmi4@gmail.com

Guide Details:

V. Lokeshwara Reddy, Associate Professor, Department of CSE, KSRM College of Engineering, Kadapa