HIDING DATA INTO THE JPEG/MP3FILE USING SBR ALGORITHM

[1]Ashwini Palimkar, [2]Prof.Dr.S.H.Patil

[1]M.Tech Scholar, [2]Professor,
Department of CSE, Bharati Vidyapeeth University COE, Pune, Maharashtra, (India)

ABSTRACT

This paper contains concept of data leakage, in every organizations, now a day’s data leakage is a critical issue facing everyone. The Information within an organization rises significantly each year which might be a point where it would be difficult to manage, resulting in data leakages.

Data leakage is also known as information leakage, when the highly sensitive data is leaked intentionally or unintentionally to unauthorized (users) parties. The information leaked out is either personal in nature or most confidential. In this case we have used Audio Steganography and image Steganography, to prevent the information leakage.

Information embedding is the beautiful way of hiding information for different formats such as, for maintaining crucial data, secure sensitive information. Standard method is the Steganography; Steganography used in digital categories as embedding file in the multimedia form , such as an image, an audio file or even a video file. This paper presents a new Steganography technique in SD for encoding extra information in an image file by denoting tiny modifications to its pixels. The proposed method focuses on one particular popular technique, Least Significant Bit (LSB) Embedding. Instead of using the LSB-1 of the cover for embedding the message, LSB-2 has been used as compared to existing algorithm as to give more security as well as to increase the robustness of data leakage detection system. and protect the data against the external disturbances as compression filter, noise..[Using SBR Algorithm For more protection to the data bits a Stegno-Key has been used to permute the message bits before embedding it. An experimental result of the proposed method shows that this system helps to successfully hide the secret data into the image file as jpeg and audio file with minimum distortion made to the image file and audio file.

We study the concept as “**Our goal is to detect when the Owner’s confidential**
(Sensitive) data have been leaked by users, and if possible to detect the user that leaked the data”.

Keywords: Steganography, Embedding Data, SBR Algorithm, Least Significant Bit, mp3&jpeg file.

I. INTRODUCTION

Information Leakage is a very serious threat facing several companies and organizations. Whether discovered by malicious attackers, unaware attacks, information loosed can damage a organization's status , reduce reputation value, and damage the organizations friendly feeling value and reputation. If any organization is doing the business in outsourcing for data processing, they have to share their data with the third person. The biggest threat is not the probably external third person not malicious person but unaware third person inadvertently divulging crucial information because more form of the data handling are being utilized within organization.

Data leakage is the transfer of some private data within an organization from user (unauthorized) to an external third person; this can be doing as using electronic concept or a physical method. In the new world of growing communication it is very important to transmit the information in a very secure manner, so that the confidential or personal information should not be leaked to third unauthorized person or party. The technique to hide the information within a system is called as steganography in simple way it is nothing but "covered writing".

It is very interesting to see how steganographic technique operates. Mainly replacing the information bits which are not used for various non visible data. The embedded data may be in various formats such as Even image, coding words (cipher txt) or also may be plane text format.

Steganography can be used in various digital records or data such as audio program, text program, video program & various images. With the help of steganography we can hide the quantum no of information because of its. low visibility factor & higher capacity to transfer the data safely to the correct person without any obstruction.

There are various algorithms in steganography for different data images frame formats.

LSB stands for least significant bit ,this program technique is used to hide large number of information in to an image form, In this case the message is replaced by least significant bit pixels. It is the most effective way to send the information easily & also in very short period of time

Steganography method uses basic terms are as, the carrier as cover image, the secret data as message, and the stegano key. The carriers such as a digital image, an mp3, or TCP/IP packet. Secret data is the information which is needed to be hidden in the suitable digital media. A stegano key is used to decode the hidden message.

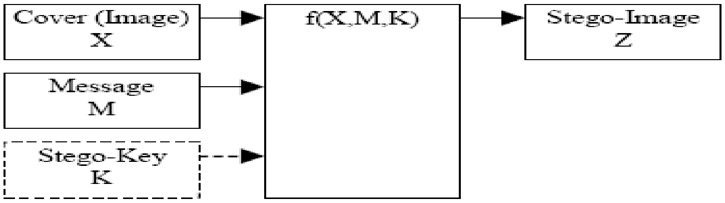


Figure 1: Basic Digital Steganography

In steganography, before the hiding process, sender must select an image file, secret data to be hidden and stegano key used as password. This paper proposes a new second bit replacement algorithm to hide data in a JPEG image/audio file using steganographic method. In this we have used Compression method to increase the hiding capacity. We have used java application as front end And SQL query processor as back end for implementing this project.

II. MOTIVATION

- First reason for selecting this method in our project as that steganography can not received little attention as it is ignored concept.
- It is not so familiar of the world.
- Want many researches to give interest in this subject.
- For researching this topic as guessed that terrorists may be planned terrorist attacks by using steganography concept to communicate with each other.
- Detect unauthorized person.
- To protect/copyright the digital work.

III. IMAGE/AUDIO STEGANOGRAPHY

3.1 Image Stegano

Images are the most popular format used for steganography concept; Images are the matrix of pixels .Pixels are known as single point. Images are of two types as 8 bit image and 24 bit image .8 bit images can be used only 256 colors and 24 bit images are used twos power 24 colors can be used There are 8 bits used to define the color of each pixel. Digital color image is stored in 24 bit Files & uses RGB color model as represents red [8 bit], green [8 bit], and blue [8 bit]. Images are too large and big, while working with larger images .It is very difficult to transmit over an open system environments. Compression method is used to shorten the size of image file displaying the correct image in time & technique using mathematical calculations which analyses compress images.

Compression ratio In this system we can compress 80% of the original image by using the mathematical calculations .In this we are embedding small amount of data. so that it is not noticeable by our eyes. We have two categories for compression methods: lossy compression method as well as lossless compression method. These methods are used to compress cover file and are used to save storage space, but they are implementing differently.

3.2Audio Stegano

MP3, as a STD for transmit the data and storage of compressed audio, is challenging cover format for steganography. MP3 is the most popular and widely used audio file format. In audio Stegnography methods, secret data is embedded in digital sound; the crucial data can embed in wav and mp3 sound files. Audio steganography method is very difficult and hard to detect method as compared to other cover media as image files, text files. In this we have used LSB -2 methods for embedding secret data in mp3 files. There are several audio steganography techniques. we can apply the compression function on mp3 file on layer3in the embedding process.

3.3 Categories of Image Steganography

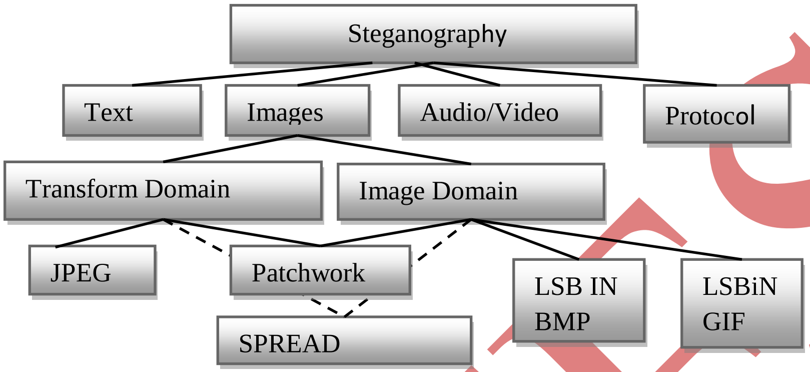


Figure 2: Categories of Image Steganography.

3.4 Steganography used in various areas

1. Image Steganography allows for two parties to communicate secretly and covertly [on the internet].
2. It allows for copyright protection on digital files using the message as a digital watermark.
3. For the transportation of high-level or top-secret documents between international governments.
4. Remarkable use in Military Applications
5. It can also dangerous in many situations. It can be used by hackers to send viruses and Trojans to destroy the machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.
6. In identity cards, embedded the detailed personal information into the jpeg image as photograph.
7. In medical field, hided details of patient treatment into image and send to authorized user so reduce time period, also cost & protect the information.
8. Stegnography is also used in safely online election in online voting system.
9. Also used for Military communication system.

IV. Proposed System

In Proposed System, We have chosen the Steganography second bit replacement algorithm (LSB-2).In this method, RGB color model, pixel value differencing concept (PVD), Compression technique, JPEG image file and audio file has been used in this algorithm. JPEG image file and audio file has been used as cover file. We can hide data upto

54223 bytes. The data is embedded in the LSB-2 of the cover image to increase the robustness of the data leakage model and to protect the data against external disturbances such as attacker filter, compression, noise.In this we have called as owner of the database as admin and faithful trusted third person are users.

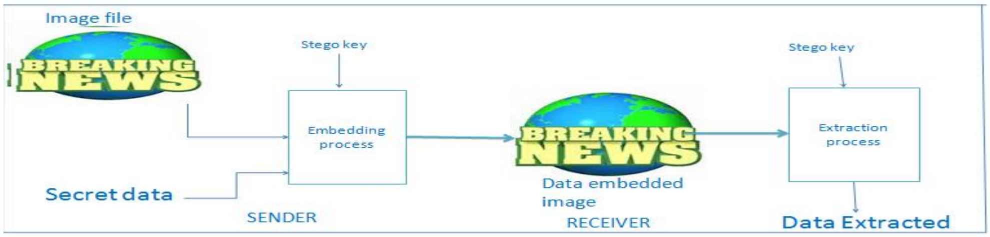


Figure 3: Proposed System.

The proposed system consists of:

Embedding Process

```
Inputs: Image file, secret data, stegano key
Output: Data embedded image
Step 1: Send the Original image and convert in binary form and store it in the array called Pixel-array
Calls the compression function
Step 2: select secret data convert it in binary and store it in the array.
Step3: select the image file and find number of pixels, set LSB-1=Ai array.
Step4: select the image file and find number of pixels, set LSB-2=Bi array.
Step 5: Encode Stegano key in binary and store it in the array
Step 6: check the length of secret data and length of image file.
Step 7: Select first pixel
Step 8: First select bit from the starting of the key array, and LSB bit form first byte of pixel.
Step 9: used SHIFT operator and AND operator.
Step 10: Start Loop1
    If bit of data to be hidden is=1& Bi = 0
        Then 1.replace value of Bi
             2. Ai=0
             3. Set as minus 1 pixel value
    End
Step 11: For second byte of image file
    Start Loop2
    If bit of data to be hidden is=0& Bi = 1
        Then 1.replace value of Bi
             2. Ai=1
             3. Set as increase 1 pixel value
    End
Step12: Replace necessary bits as defined by Compression ratio in each pixel, Store information about bits Embedded in binary file.
Step13: Repeat step8, step9, step10, step11, step12 6 till all the bits of image file has been embedded.
```

. Extraction Process

Inputs: Embedded image file, Stegano key
Output: Secret data
Step 1: Select the path in which you want to extract the embedded data
Step 2: Select the embedding image file.
Step 3: Apply security key.
Step4: Convert the binary file into human understandable form.

Fig4 (a) shows the original sports image the data is embedded in it. Fig4 (b) shows the data embedded in the image. It should be noted that original sports image and data embedded sports image are exactly same.

Secret data used in our method is shown below", using steganography (way of hiding data) and SBR algorithm, we can 100% detect the guilty agent. Here Stegno key used in this algorithm, Is as USERNAME (which is Unique).

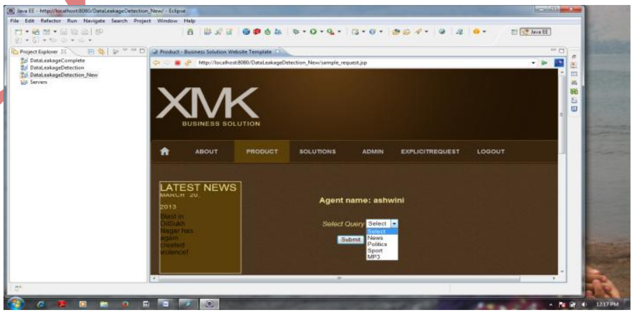
In this, Guilty agent leaks the sports news from the BNN news channel, this agent name is ashwini.

Using proposed method the admin detect this agent as shown below,

"sports_INDASHWINI", So here guilty agent is "ASHWINI."

The flow of our system is given as below:

- User's Request: Explicit or sample
- Leaked dataset given as an input to the system.
- The list of all users having common records as that of leaked records is found.



Java EE - http://localhost:8080/DataLeakageDetection_New/ - Eclipse

http://localhost:8080/DataLeakageDetection_New/sample_request.jsp

LATEST NEWS
MARCH 20.
2013
Blast in DilSukh Nagar has again created violence!

Agent name: ashwini

Select Query: Select

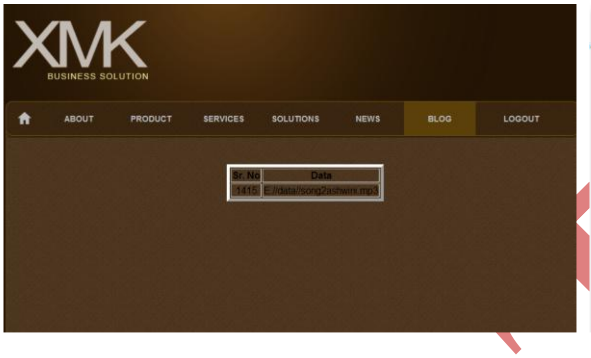
Figure 5: Agent requesting sample request

Here agent can request sample or explicit. Agents are selected as sample request as MP3 file.

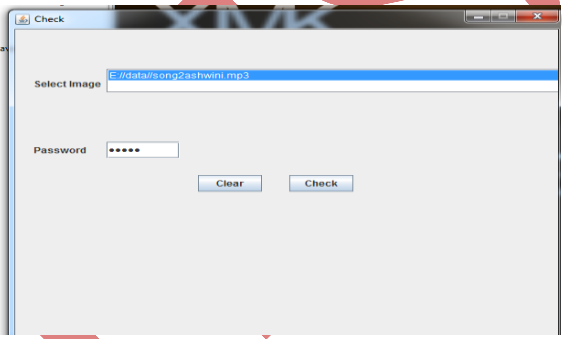
Path as "E://data//song2.mp3"[before embedded data]

Path as "E://data//song2ashwini.mp3"[after embedded data]

The proposed technique is simulated in java with the data and audio files. The data is encrypted and is embedded into the audio file then that audio file is encrypted. By using this technique we find no difference in the size and the quality of the audio file before embedding data and after embedding data.



Sr. No	Data
1415	E://data//song2ashwini.mp3



Select Image: E://data//song2ashwini.mp3

Password: •••••

Figure6: Leaked MP3 file by Agent

Figure 7: selection path of leakage MP3 files

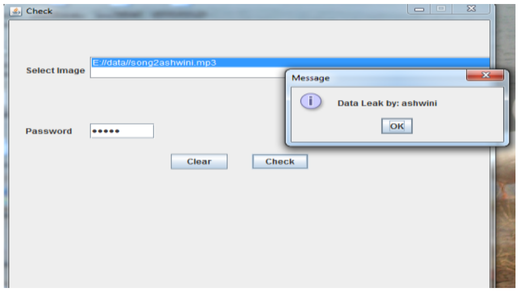
Table 1: Comparison between LSB method and proposed method [SBR]

Table 2. System supports following file formats

Method/Images	**Simple LSB method**	**SBR method**
News_hindi.jpeg	50.08	53.35
Politics.jpeg	49.23	52.06
Sports_india.jpeg	49.45	52.44

File Formats	**Secret Msge**	**Embedding**	**Extraction**
Jpeg image	Text Message	Done	Done
Mp3 File	Text Message	Done	Done
Text File	Text Message	Done	Done
Bmp file	Text Message	Done	Done

As compared to simple LSB method, proposed SBR method is greater PSNR value



Select Image: E://data//song2ashwini.mp3

Password: •••••

Data Leak by: ashwini

Figure 8: Data leakage can seen agent Guilt

VI. CONCLUSION

From this above discussion, we conclude that the data leakage detection system model using Stegnography concepts is very useful as compare to an existing system. In many cases, we have not totally sure with work of users that have not be hundred percent depends and we cannot have dependency if a leaked data record came from an user or from other way, since certain data cannot attempt watermark concept. To overcome this problem we have used as Stegnography method, simply means “CoveredWriting”.this technique provides the complete security against “Data Leakage”. In this paper we have proposed the use of SBR algorithm to embed the given secret data into the image file as JPEG and hide the data in MP3 files.

JPEG images’ mostly used for Stegnography applications because they are popular as compared to other image format and also securely /privately communicated over an open system environments like Internet. We have used algorithms as explicit and sample, using embedded data data owner can increase chances of identifying a leaker. We have also used an compression technique. We have developed system in java based on proposed algorithm.

Here we have tested several JPEG images and mp3 files with secret data hidden and we can concluded that resulting data embedded image do not have any noticeable changes.

REFERENCES

[1] A.E.Mustafa, A A. M.Elgamal, M.E.Elami, Ahmad bd, ”A proposed Algorithm For Steganography in Digital image Based On LSB” Research Journal Specific Education Faculty of specific Education, Mansoura University, Issue no. 21, April. 2011.

[2] Vijay Kumar Sharma, Vishal Shrivastava “Steganography algorithms for hiding image in image by improved lsb substitution by minimize detection” ,in Journal of Theoretical and applied Information Technology15th February 2012. Vol. 36 No.1.

[3] Alain, C. Brainos, A Study of Steganography and the Art of Hiding Information, East Carolina university.

[4] Desoky, A. (2009):A novel Noiseless Steganography paradigm, Ph.D., Department of Computer Science and electrical engineering, Faculty of the Graduate School, university of Maryland, Baltimore County.

[5] Christopher, T. (2007): Compression Aided feature Based steganalysis of Perturbed Quantization steganography in Jpeg image, M.Sc. s, Department of science in Electrical and Computer Engineering, University of Delaware.

[6] Xiang-yang, L. , Dao-shun., Ping, W., Fen-lin, L.((2008): a review on Blind Detection for Image Steganography, journal of Signal Processing, Vol(88),Issue(9).

[7] Samer, A.(2006):A New Algorithm for Hiding Gray Images using Blocks, Information , Security Journal, The hashemite University, Jordan, Volume (15), Issue (6).

[8] Kaushal M. Solanki, 2005, Multimedia Data Hiding: From fundamental Issues to Practical Techniques, PhD, electrical and Computer Engineering, university of california, Santa Barbara.

[9] Sanjeev, M.et.al (2008): Customized and Secure Image Steganography, Journal of Signal Processing, Vol (1), Issue (1).

[10] Hengfu, Y., Xingming S., Guang S(2009): A High- capacity Image Data Hiding Scheme Using adaptive LSB substitution, Journal of radio engineering, vOL. (18), NO. (4).

[11] Lee, L.(2004) :LSB Steganography :Information within Information, Journal of Computer Science, Vol (265), N(5).

[12] Amirthanjan, R.Akila, R & Deepika chowdavarapu,a Comparative Analysis of Image steganography', 2010.

[13] Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image.international Journal of Advancements in Technology, 1(1), pp.05-11.

[14] Kaur, R. Dhir, & G. Sikka. (2009). A new image steganography based on first component alteration technique. International Journal of Computer Science and Information Security (IJCSIS), 6, 53-56.

[15] TMorkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the fifth Annual Information Security South Africa Conference,(ISSA2005), Sandton, South Africa, june/July 2005.

[16] Robert Krenn, " Steganography and steganalysis", Internet Publication, March 2004.

[17] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[18] Petit colas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking.", 2000.

[19] Alain, C. Brainos, A Study Of Steganography And The Art Of Hiding Information, East Carolina University.

[20] J.L.Dugelay and S.Roche, "Information Hiding: Techniques for Steganography and Digital Watermarking", S.Katzenbeisser and F.A.P.Petitcolas (eds.), Norwood, MA: Artech House, pp. 121-148,

[21] Ajanthaa lakkshmann, Puja u.dharia, Fairy Gandhi, An adaptive image steganography technique using LSB and MSB international research journals V3, n1, 2013, ISSN 1839-6518.

[22] Jain, Sachin Mesh ram, Shikha Dubey, Image Steganography Using LSB and Edge detection Technique", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-3, July 2012.

[23] TMorkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[24] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[25] Yang, C.-H.: "Inverted pattern approach to improve image quality of information hiding by LSB Substitution", 2008.