DOUBLE CODING MECHANISM FOR ROBUST DATA TRANSFER

N.Ramya¹ | D.Rukmani¹ | V.Subhangini¹ | Mrs. S. Yuvarani²

¹(U.G Scholars, Dept. of Electronics and Communication Engineering, V.S.B Engineering College, Karur) ²(Dept. of Electronics and Communication Engineering, Assistant Professor, V.S.B Engineering College, Karur)

Abstract— In this paper we are using two types of coding mechanism such as pseudo random code and Morse code. It is considered to be simple and lusty method since the above summarized techniques have been implemented in same audio data which is hided. Our proffered method provides satisfactory results for transmitting the message in a guaranteed way. In addition to the security, it is also a reliable process since the hidden message is embedded into a video file. The performance of this method is evaluated using MSE (Mean Square Error) and PSNR (Peak to Signal Noise Ratio). In our paper the audio and video installation is done with the help of compression technique and in the meanwhile it doesn't affect the quality of the veiled audio.

Keywords— Morse Code; Pseudo Random Code; Double Coding; Stegnography; Embedding; Extraction

1. INTRODUCTION

Stegnography is the process of concealing messages or information within other non-secret text or data. In our proposed method, this stegnography approach plays a vital role. It has been used in many applications such as audio video synchronization, TV broadcasting, in defense forces, Media Database systems, copyright control, Confidential communication and secret data storing and digital watermarking etc. In stegnography process, the media file to be hided is enclosed by the another media file which can be an image, music or video. The media file which is used to protect the original information is known as cover media. The embedded data is said to be stegno file and at the same time we should be aware whether the stegno media has the information or not. This encrypted file should not be easily analyzed and visible by the other file.

Stegnography is one of the encryption technique that can be used along with the cryptography as an ultrasecure method to protect the data. It is derived from the Greek word "stegnos" means covered and "graphie" means writing.

2. CURRENT ISSUSES

A short time ago, everything is contributing in the direction of digitization and also with the reinforce of internet technology. Digital media can be put on the air quickly over maze. For suppressing mysterious information in an illustration, there endure a large collection of steganography techniques, some are more tangled than others. So, we strengthen this application to make the data more screening and also naturally and convenient.

3. FUTURE PROCESS DUE TO THIS SOLUTION

The progression approaching electronic communication and humans desire to cloak message from examining their belief with expeditious upgrading technology. Steganography software is more effective in covering data in audio, video format. Actually, what Steganography essentially does is exploit human perception because human senses are not trained to look for files.



fig(a). Steganography application scenario

There are three common fundamentals named as security, capacity and imperceptibility used to determine the rate conduct quantum of steganogaphy techniques. To embed well known peak to signal ratio categorize under distortion metrics applied are given as,

$$PSNR = 10\log_{10}\left(\frac{r^2}{_{MSE}}\right)$$

4. PROPOSED METHOD

In our proffered paper, wavelet technique have been established instead of the LSB method. In LSB, only the least significant variables have been encrypted and transmitted. Since this methodology is so simple and easily decrypted by the growing technology. So we introduce this wavelet process in hiding of information. Here, we mainly concerned with hiding audio in videos, that is using of two coding mechanisms on same data after performing wavelet transform and exposing the stego videos to compression technique. Discrete Wavelet Transform (DWT) is the main principle algorithm handled in this paper. Haar wavelet type is used in DWT.



5. BLOCK DIAGRAM OF PROPOSED SYSTEM



6. EXPLANATION OF BLOCK DIAGRAM

For covered writing, a sample video file of any length can be selected. The standard AVI format (audio video interleave) is preferred as audio and video are going to be embedded. The video can be segmented into frames. The quality of video will be more when it has more number of frames. Color conversion is performed after framing process where RGB is changed into YUV. Luminance component 'Y' is preferred. For conversion the following formulae can be employed.

```
Y=0.299R+0.587G+0.114B
U=-0.147R-0.289G-0.436B
V=0.615R-0.515G-0.100B
```

Discrete wavelet transform is compiled for the input media which is to be discretely sampled. The audio file to be shrouded is taken in waveform audio file format (wav). For geminate coding mechanism Pseudo code and Morse code are used. Pseudo codes can be generated by linear feedback shift registers. It is also called as coarse acquisition code. Then the corresponding ASCII code is found for the pseudo random codes. Morse code is used in telegraph system where dots and dashes are in series. It is applicable for alphabets and numbers. The vectorized audio file is blocked by double coding. The audio and video is embedded. This technique is contemplated as an immune way to transfer our information. It can provide distinct and exclusive haphazardness in each code. Then inverse wavelet transform is performed for the embedded file. Video is compressed after the color conversion process.

Research script | IJRE Volume: 05 Issue: 02 2018 During color changeover 'YUV' components are converted into 'RGB'. The pixel range of RGB is 0 to 255. Similarly for this conversion the following formulae can be exerted. R=Y+1.140V

G=Y-0.395U-0.581VB=Y+2.032UThe stego video file can be obtained finally.

7. ALGORITHM

1. For Encryption

STEP 1: Select the video file STEP 2: Conversion of RGB to YUV frame STEP 3: Discrete Wavelet Transformation is performed on the converted frames

$$y_{low}[n] = \sum_{k=-\infty}^{\infty} x[k]\dot{g}[2n-k]$$

$$y_{\Box ig\Box}[n] = \sum_{k=-\infty}^{\infty} x[k] \dot{\Box} [2n-k]$$

STEP 4: Generation of pseudo random code and morse code to encrypt the audio files are evaluated by using the formula

$$x_{n+1} = (ax_n + c) \mod c$$

Where,

m-modulus

a-multiplier

c-increment

x_n-seed or start value

STEP 5: Embedding the encrypted audio in video file

STEP 6: Conversion of YUV to RGB frames by the below mentioned formula

- R = Y+1.140 VG = Y-0.395U-0.581V
- B = Y + 2.032V

2. For Decryption

STEP 1: Select the stego video files

STEP 2: Perform the frame and color conversion RGB to YUV

STEP 3: Perform the Discrete Wavelet Transform

STEP 4: Decrypt the audio using pseudo random code generation and morse code conversion

STEP 5: Data extraction from the video files

From the above mentioned procedures we can encrypt and decrypt the hidden informations efficiently. Hence, the datas are more secured in the embedded form.

3. Pixel conversion

Cover image is represented in YCbCr channel. Then using clustering modification transformation approach which is a decomposition of a function into a linear combination of the spatial features. The inverse wavelet transform shows that the original signal may be synthesized by summing up all the projections of the signal onto the spatial basis. In this sense, the continuous transform behaves like an orthogonal transform. Lifted wavelet transform approach RESEARCH SCRIPT

which uses integer to integer transformation which is implemented using lifting wavelet transformation (LWT). LWT uses Lifting Scheme (LS). In LS, among the various wavelets available, appropriate wavelet is chosen. As integer coefficients are required, 'int2int' transformation has to be specified. Based on the LS, apply the LWT to cover audio to get detail and approximation coefficients, CD and CA respectively. Convert CD to binary. And also do the same process in audio signals.

4. RGB

- The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors.
- The name of the model comes from the initials of the three additive primary colors, red, green, and blue.
- The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems, such as televisions and computer, though it has also been used in conventional photography. Before the electronic age, the RGB color model already had a solid theory behind it, based in human perception of colors.
- RGB is a device-dependent color model: different devices detect or reproduce a given RGB value differently.

5. CMYK

- The CMYK color model (process color, four color) is a subtractive color model, used in color printing, and is also used to describe the printing process itself.
- CMYK refers to the four inks used in some color printing: cyan, magenta, yellow, and key (black). Though it varies by print house, press operator, press manufacturer, and press run, ink is typically applied in the order of the abbreviation.
- The "K" in CMYK stands for key because in fourcolor printing, cyan, magenta, and yellow printing plates are carefully keyed, or aligned, with the key of the black key plate.
- Some sources suggest that the "K" in CMYK comes from the last letter in "black" and were chosen because B already means blue. However, this explanation, although useful as a mnemonic, is incorrect.
- The CMYK model works by partially or entirely masking colors on a lighter, usually white, background. The ink reduces the light that would otherwise be reflected. Such a model is called subtractive because inks "subtract" brightness from white.

8. CONCLUSION

We concludes that hide the audio in video for privacy preserving requirements. Our proposed system use the clustering modification strategies approach to embed audio in video. The proposed method can take advantage of all traditional data hiding techniques for plain videos and achieve excellent performance without loss of perfect

Research script | IJRE Volume: 05 Issue: 02 2018 secrecy. Furthermore, this novel method can achieve less payload, separate data extraction and greatly improvement on the quality of marked stego images. The information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change)

REFERENCES

- J. J. Chae and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients," University of California, Santa Barbara, CA 93106.
- [2] Yun Q. Shi, "Reversible Data Hiding," New Jersey Institute of Technology, Newark, NJ 07102, USA.
- [3] Kamrul Hasan Talukder and Koichi Harada, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image,"
- [4] Musbah J. Aqel , Ziad A. Alqadi , Ibraheim M. El Emary, "Analysis of Stream Cipher Security Algorithm," Journal of Information and Computing Science, ISSN 1746-7659, vol. 2, no. 4, 2007, pp. 288-298.
- [5] S.Imaculate Rosaline, C. Rengarajaswamy, "A Steganographic Substitution technique using APPM for encrypted pixels".
- [6] Sapna Sasidharan and Deepu Sleeba Philip, "A Fast Partial image Encryption Scheme with Wavelet transform and RC4," International Journal of Advances in Engineering & Technology, ©IJAET ISSN: 2231-1963.
- [7] Manikandan R, Uma M, "Reversible Data Hiding for Encrypted Image," Journal of Computer Applications ISSN: 0974 – 1925,vol. 5, Issue EICA2012-1, February 10, 2012
- [8] C. Rengarajaswamy, K. Vel Murugan, "Separable Extraction of Concealed Data and Compressed Image,".
- [9] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.
 [10] L. Luo et al., "Reversible image water marking using
- [10] L. Luo et al., "Reversible image water marking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.