ABSTRACT:

Steganography is a technique used to hide the secret data within cover media. Cover media types can take many forms such as text, audio, digital images, and video. Earlier research has been done mostly on text and image steganography due to their popularity on the internet. In this paper, the method of concealing an image, individually, on multiple frames of a video, using DWT Algorithm is proposed. Experimental results prove that our proposed method.

Keywords: Video Steganography, Data hiding, DWT, Mid-Prime, PSNR, MSE

[1] INTRODUCTION

Steganography is the art of hiding information in original files in such a way that the existence of the message cannot be known. The term Steganography comes from Greek word Steganos, which means, “Covered Writing”. Nowadays most of the applications is Internet-based and in some cases it is desired that the communication be made secret. There are two techniques available to reach this goal. One is cryptography, where the sender uses an encryption key to encrypt the message, and this encrypted message is transmitted through public channel, and decryption algorithm is used to decrypt the message. The restoration of the original message is possible only if the receiver has the decryption key. The second method is Steganography, where the secret message is inserted in a new medium. The original files can be referred to as cover image. A stego-key is used for hiding process to limit detection and/or recovery of the embedded data. Steganography is different from Cryptography. The purpose of cryptography is to secure communications by changing the data into a form that cannot be understood, where as Steganography techniques, hide the existence of the message itself,
which make it difficult for a third person to find out where the message is. Sometimes sending encrypted information may arouse suspicion, while invisible information will not. Both techniques can be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well. The process of cracking of Steganography messages is called steganalysis. The purpose of steganalysis is to identify the information and determining that whether or not they have secreted messages encoded into them and if possible, extract the hidden information [1]. Steganography system can be categorized into spatial and transform domain methods. In spatial domain, the processing is applied on the image pixel values. In the transform domain method, the first step is to transform the cover image into spatial domain. Then the transformed coefficients are processed for hiding the secret information. The image after the embedding of the secret message, so-called stego-image, is then sent to the recipient over a public channel. In the transmission process, the public channel may be intentionally monitored by some opponents who try to prevent the message from being successfully sent and received.

Discrete Wavelet Transform:

The wavelet transform describes a multi-resolution composition process in terms of expansion of an image onto a set of wavelet basis functions. DWT is the multi resolution report of an image. DWT split the signal into high and low frequency parts. The low incidence part is split again into high and low frequency parts, while the high frequency part contains information about the frame components. DWT transform is applied to an image it is decomposed into 4 sub bands: LL, HL, LH and HH. To perform a second level decomposition, again DWT is applied to LL1 which decomposes the LL1 band into the 4 sub bands. Fig 3 shows a second level decomposition. Haar Transform decomposes each signal into two components, one is called average (approximation) or leaning and the other is known as difference (detail) or changeability.

DWT is used for digital image. Many DWT’s are available depending on the application most appropriate one should be used to hide test message integer wavelet transform can be used. When DWT applied to an image it is decomposed into four sub bands, LL, HL, LH, and HH.

The LL part contains the most significant features and so, if the information is hidden in LL part of the stego image compression or other manipulation may produce distortion. So, normally data is hidden in other bands of transformed image. In compression multi resolution property of DWT is suitable for transmission of image and video data.

Haar –DWT:

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the even horizontal and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:
Haar wavelet operates on data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One important feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner.

**Figure: 2. The horizontal operation on the first row**

**Step 1:** At first, pixels are scanned from left to right in horizontal direction. Then, perform the addition and subtraction operations on next pixels. Store the sum on the left and the difference on the right as illustrated in Figure 1. Repeat this operation until all the rows are processed. The pixel sums characterize the low frequency part (denoted as symbol L) as the pixel difference represents the high incidence part of the original image (denoted as symbol H).

**Step 2:** Secondly, check the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the diversity on the bottom as illustrated in Figure 3. The process is repealed until all the columns are processed. Finally we obtain 4 sub-bands denoted as LL, HL, LH, and HH in that order. The LL sub-band is the low frequency portion and so looks very similar to the original image.

**Figure: 3. The vertical operation**

The entire process described above is called the first-order 2-D Haar-DWT. The first-order 2D Haar-DWT applied on the image “Lena” is illustrated in Figure 4.

**Figure: 4. Discrete Wavelet Transform**

[2] RELATED WORKS

Abhinav Thakur et al. (2015) [1] deals with data hiding technique in which the secret data is embedded into the cover video. Firstly, cover video is decomposed into different
frames. A single level Discrete Wavelet transform is applied on selected frame and on secret image. A private key is used during the process of encoding and decoding to provide high security.

Nasraddin Ahmed Salem Al-Maweri et al. (2016) [2] proposed an efficient method to hide the metadata of UAVs (Unmanned Aerial Vehicles) video using the technology of digital watermarking Discrete Wavelet Transform (DWT) is used to implement the embedding of the information robustly. In addition, a new scrambling algorithm is proposed to secure the information before hiding. The experimental results prove the high performance of the proposed method.

Said E. El-Khamy et al. (2016) [3] proposed an efficient steganography scheme based on sample comparison in Discrete Wavelet Transform (DWT) domain where the cover audio is decomposed into several multi sub-bands, and then selected coefficients of details are changed by a threshold value depending on the embedding cipher image bit. This approach employs an original image component to perform RSA encryption on it, and then cipher bits are embedded in the details components of the audio signal according to a predetermined threshold value.

Po-Yuen Chenet et al. (2006) [4] proposed a new steganography technique which embeds the secret messages in frequency domain. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Some basic mathematical operations are performed on the secret messages before embedding.

M. Mary Shanthi Rani et al (2015) [5] proposed a method to hide and share multiple multimedia data in an efficient and secured way. The proposed secret sharing process includes 3 phases: Encryption, Steganography and Visual Cryptography (VC). The first phase encrypts the secret message to be communicated into a cipher text using XOR method. The second phase is used to hide the cipher text dynamically in an image by changing the number of bits hidden in RGB channels based on the indicator value. The basic idea of VC is to split original secret images into several partitions which are also called shares. In the final phase four shares are created from a secret image and simultaneously the stego image created in the previous phase is hidden in these shares. By increasing the number of shares we can store more number of stego images thereby the amount of secret data are very safe because separately they reveal nothing about the multimedia content hidden in then transmitted across the network increases multi fold. The secret image, stego images and the hidden messages can be recovered from the shares without involving any complex computation.

M. Mary Shanthi Rani et al (2015) [6] proposed a technique. It consists of two phases. The first phase is used to hide the message dynamically in a Cover Image1 by changing the number of bits hidden in RGB channels based on the indicator value. VC schemes conceal the Cover Image2 into two or more images which are called shares. In the second phase two shares are created from a Cover Image2 and the stego image created in the first phase is hidden in these two shares. The shares are safe as they reveal nothing about the multimedia content. The Cover Image2, stego image and the hidden message can be recovered from the shares without involving any complex computation.
M. Mary Shanthi Rani et al (2016) [7] proposed a novel method to authenticate so that only shares from authorized users are combined to reveal the secret image. This is done by first embedding QR Code (abbreviated from Quick Response Code) into the secret image, followed by the creation of shares. The original secret image is not affected as we embed the QR Code in non-region of interest. If a modified share or unauthorized share is superimposed on to the original share, the embedded QR Code cannot be read/retrieved from the resultant image. This signifies that one of the shares is not an authorized one. In VC the reconstructed image, encounter a major problem of pixel expansion. This is also solved in their proposed method by compressing the shares using a hybrid method that combines Vector Quantization and Run Length Encoding methods to achieve lossless compression. Decompression is done by applying decoding procedure and the shares are overlapped to view the secret image.

Anupriya Sohal et al. (2015) [8] After the embedding procedure, the resultant object i.e. the stego object is quiet good in quality with respect to visibility. In extraction procedure it has been aimed to extract the original message intact which has been executed successfully by the above mentioned extraction algorithm.

Nishi Khan et al. (2004) [9] the proposed system is more effective for secret communication over the network channel, as key frame extraction method would not be known to hackers as it is completely new technique for video steganography, which is the main strength of my proposed method, so they will not be able to find data hidden frames easily.

Manisha et al. (2016) [10] propose a new steganographic method for transmitting digital images based on discrete wavelet transform using two different techniques. A Technique used for three level wavelet decomposition taking the single plane of cover image for embedding and processing cover image as 4x4 blocks with swapping and another technique used single level decomposition.

M. Mary Shanthi Rani et al (2015) [11] aim to hide message in spatial domain with more security. A technique is proposed to hide the message dynamically by changing the number of bits hidden in RGB channels based on the indicator value. The proposed technique attempts to overcome the problem involved in sequential hiding and produces extremely low visual distortion which is imperceptible to human visual system.

M. Mary Shanthi Rani et al (2016) [12] proposed for secret communication by combining the concepts of Steganography and QR codes. The suggested method includes two phases: (i) Encrypting the message by a QR code encoder and thus creating a QR code (ii) Hiding the QR code inside a colour image. This hiding process embeds the quantized QR code so that it will not make any visible distortion in the cover image and it introduces very minimum Bit Error Rate (BER). The proposed method has high imperceptibility, integrity and security.

Mohit Gupta et al. (2012) [13] proposed the secret message is encoded before embedding in order to increase the capacity of the proposed data hiding system. The main advantage of this method is that at the time of extraction there is no requirement of the original cover image which increases the security of proposed steganography system.

Kousik Das gupta et al. (2012) [14] the proposed technique is compared with existing LSB based steganography and the results are found to be encouraging. An estimate of the
embedding capacity of the technique in the test video file along with an application of the proposed method has also been presented.

M. Mary Shanthi Rani et al (2016) [15] They focus DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and IWT (Integer Wavelet Transform) secret data are embedded inside a video file using both the methods, spatial and frequency, and the outcomes are analysed and compared. Results are compared based on PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), BER (Bit Error Rate) and Standard Deviation.

Jigar Makwana et al. (2016) [16] proposed paper the focus is on increasing data security using dual steganography. In dual steganography secret message is first embedded into cover medium and then resulted stego-object will be again embedded into other cover medium.

MohMohZan et al. (2013) [17] proposed a method to improved the image quality and imperceptibility. Our method sustains the security attacks. Proposed system presents our new insertion technique which embeds the secret messages in frequency domain. It can measure the quality of container image with secret image after image hiding process PSNR values.

Vipula Madhukar Wajgade et al. (2013)[18] Here a more secure and effective hash-based algorithm that uses a pure hash technique for coding and decoding the information in a colour image. An improved LSB (least Significant bit) based Steganography technique for images imparting better information security.

M. Mary Shanthi Rani et al (2015) [19] patient information is also embedded within the medical images, it is very important to maintain the confidentiality of patient data. Hence, this article aims at hiding patient information as well, within the medical image followed by joint compression. The hidden data and the host image are absolutely recoverable from the embedded image without any loss.

M. Mary Shanthi Rani et al (2017) [20] proposed to hide the data in both Region of Interest (ROI) of medical images and Non Region of Interest (NROI) of medical images and recover the data as well. Medical image and hidden data are recoverable without any loss of data.

3 PROPOSED METHOD

DWT haar method is used to hide the secret message within cover media. The proposed method involves two methods: embedding and extraction. In embedding process, a video is used as cover frame, which hides the secret message in selected frames using mid-prime method. Next secret data values are converted to normalized form and the normalized data is hidden in the image using DWT technique get stego image. The stego frames are then combined to form the stego video. In Extraction process stego video is converted into frames and the stego frames are selected using mid-prime technique and inverse DWT is applied to restore the message.

A. Embedding Process

In this embedding process, set of image frames are separated from cover video and mid-prime technique is applied for selecting a frame. In Mid-Prime technique, the prime numbers within the limit (limit is number of frames). Is listed out and the middle value of the prime number list is selected as cover frame number. The frame for hiding data is selected using this cover frame number. After selecting the cover frame from video, secret data are converted into
normalized form and dwt technique is applied to hide the data and get stego frame. Next stego frames are combining into stego video.

**B. Extraction Process**

In this extraction process, stego video converted into frames and select frame using mid-prime technique. After that dwt technique is applied in selected frame and original data is extracted from that frame.

---

**Flowchart Description**

1. **Start**
2. Read the input video
3. Video convert to frame
4. Select the frame using mid-prime techniques
5. Read the secret data
6. Convert secret data to ASCII value
7. Convert ASCII value to normalized
8. Decompose the cover frame by using Haar 2-level DWT
9. Embed the decomposed image
10. Stop

11. **Start**
12. Read the stego video
13. Select the frame using mid-prime techniques
14. Decompose the cover frame by using Haar 2-level DWT
15. Extract the normalized data
16. Denormalized the extract data
17. Apply inverse DWT and get original image
18. Decompose the cover frame by using Haar 2-level DWT
19. Covert all frames to video
20. Stop
**VIDEO STEGANOGRAPHY USING MID-PRIME AND DISCRETE WAVELET TECHNIQUE**

**Data Embedding**

*Figure: 5. Embedding and Extraction flow chat*

**Algorithm for embedding process:**

- Step 1: Read the video
- Step 2: Select the frame using Mid-Prime technique
- Step 3: Read the Secret data
- Step 4: Convert secret data into its ASCII value
- Step 5: Convert ASCII values into normalized form
- Step 6: Decompose the cover frame by using Haar 2-level DWT
- Step 7: Embed the normalized data into decomposed cover image

**Data Extraction**

**Algorithm for extracting process:**

- Step 1: Read the stego video
- Step 2: Select the frame using Mid-Prime technique
- Step 3: Decompose the cover frame by using Haar 2-level DWT
- Step 4: Extract the normalized data
- Step 5: Demoralized the extract data
- Step 6: Apply inverse DWT and get original image
- Step 7: Display the values of parameters PSNR and MSE between cover image and stego image and also represent the graphs of PSNR and MSE value

**[4] RESULTS AND DISCUSSION**

This section presents the experimental results of the proposed method. Table 1 Experiments are conducted on test video files for assessing the performance of the proposed method. Table 1 provides the resolution, number of frame and size of the video files used.

<table>
<thead>
<tr>
<th>Video file</th>
<th>Resolution W x H</th>
<th>No. of Frames</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vid.avi</td>
<td>480 x 480</td>
<td>484</td>
<td>2.35MB</td>
</tr>
<tr>
<td>elemp.avi</td>
<td>240 x 320</td>
<td>114</td>
<td>1.00MB</td>
</tr>
<tr>
<td>cbw.avi</td>
<td>240 x 256</td>
<td>185</td>
<td>377KB</td>
</tr>
</tbody>
</table>

The quality of stego image produced by the proposed method has been tested exhaustively based on various image similarity merits namely PSNR Peak signal-to-noise ratio, often abbreviated PSNR. It is the measure of quality of the frame by comparing the cover frame with the stego frame. MSE Mean Square Error is used to measure the distortion between cover frame and stego frame. This two terms deal with variation in video frame due to encoding.
Table 2 presents the performance comparison of the proposed method with similar existing methods in terms of PSNR, MSE and size of hidden message.

Table 2. Comparison Result for PSNR & MSE Values

<table>
<thead>
<tr>
<th>Video file</th>
<th>Vid.avi</th>
<th>Cbw.avi</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR (Existing method)[21]</td>
<td>60.21</td>
<td>54.39</td>
</tr>
<tr>
<td>MSE (Existing method)[21]</td>
<td>0.061</td>
<td>0.236</td>
</tr>
<tr>
<td>PSNR (proposed method)</td>
<td>68.2573</td>
<td>0.0097</td>
</tr>
<tr>
<td>MSE (proposed method)</td>
<td>56.8413</td>
<td>0.1346</td>
</tr>
<tr>
<td>No.hidden Character</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

It is obvious from Table 2 that the proposed method produces high PSNR values of 68.25 and 56.84 for vid.avi and cbw.avi respectively. It is also worth noting that the proposed method has achieved PSNR gain of 8 decible over the existing method for vid.avi file. Our proposed method gives very small MSE and large PSNR which is our objective that indicate that distortion after encoding secret text in video is minimal.

[6] CONCLUSION

This technique of hiding a particular text file in the video hide it securely with minimum mean square error and hence gives maximum PSNR. So it helps to transmit data securely by embedding it in a video file and without disclosing to the unintended receiver and without any alternation in secret message. The proposed technique is applied to AVI file. In future, video format other than AVI format can also be used with some modification and secret images can also be hidden in the video for secured transmission.
REFERENCES


M.Mary Shanthi Rani, S.Lakshmanan and P.Saranya 189
   technique for video steganography”, International Journal of Security, Privacy and Trust
   Management, Vol. 1, No 2, April 2012.

   Steganography in Spatial and IWT Domain”, International Conference on Advances in

   Digital Communication”, International Journal of Advanced Research in Electrical,

   Discrete Wavelet Transform”, International Journal of Engineering Research & Technology,
   Vol. 2 Issue 8, August - 2013

[19] Vipula Madhukar Wajgade, Dr. Suresh Kumar, “Enhancing Data Security Using Video
   Steganography ”, International Journal of Emerging Technology and Advanced Engineering

   Compression of Medical Images” International Journal of Advanced Information
   Technology (IJAIT) Vol. 6, No. 1, February 2016

[21] M. Mary Shanthi Rani and S. Lakshmanan, "Region Based Data Hiding in Medical
   Images”, International Journal of Advanced Research in Computer Science, vol. 8 , No. 3
   March – April 2017

[22] Dr. P. R. Deshmukh and Bhagyashri Rahangdale, "Data Hiding using Video
   4, April - 2014