STEGO Hamming Based Data Security in Image Processing Applications

Vipparla Rama Rao

Associate Professor, Department of ECE, Eluru College of Engineering and Technology, Eluru, India.

ABSTRACT

Due to rapid increase of exchange of large data with technological advancements, video steganography is becoming the better solution for offering greater security for large data. In this paper, an enhanced and secured video steganography algorithm is proposed. Hamming code encoding technique and embedding process in DWT domain are the main key concepts used for the project. At embedding phase, initially secret message is secured by encrypting using a key. Then the secret message is encoded using Hamming code. To ensure furthermore security, secret message is XORed with the random value generated by a private key. The processed secret message is then embedded into middle and high frequency DWT coefficients of selected frames of video. For extraction, reverse process takes place. However, for extracting the secret message, keys should be known. This additional feature of using keys makes the technique more robust. The performance parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are calculated to determine the quality of stego video. The obtained results have shown that the proposed algorithm for steganography is highly secured with good perceptual invisibility.

KEYWORDS: Steganography, Hamming code, DWT, Embedding Process.

I. INTRODUCTION

Secured information transfer has become really challenging nowadays because of advancements in technology and availability of high speed internet. Steganography provides the solution for secured communication. Steganography is the science of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word [1].

Characteristics for a steganographic scheme:

Depending on the results obtained for the following parameters a steganographic technique can be judged [1]. The parameters are:

a) Capacity: The amount of data that can be hidden.

b) Undetectability: Inability for the computer to use any computational methods to differentiate between cover object and stego-objects.

c) Robustness: Ability of the technique to retain message's originality after detection.

d) Security: A steganography algorithm or technique is said to be secured if the hidden information cannot to be removed or retrieved by the intruder even after the presence of message is identified.

Video Steganography: A process of hiding any type of secret file in a video refers to video steganography. Due to the advent of internet and its fast speed, hiding of images has gain more importance, as images convey useful information pictorially. Video steganography takes the advantage of fast moving of frames of a video as Human Visual System (HVS) can't detect the change in fast moving objects. Many techniques have been proposed for video steganography [2]. Mostly, these techniques fall under following categories:

a) LSB approach b)Masking-filtering c)Transformation techniques

a) LSB approach: The simplest approach for hiding secret message in a video. The procedure involves hiding the message bits into the least significant bits of the chosen cover frame. Modification of LSB's results in smaller changes and are left unidentified by HVS. So it remains the simplest approach and less complex technique. However care should be taken in choosing the number of LSB's to be modified. Increasing the changes over LSB's increases the capacity, however it degrades the cover frame's quality.

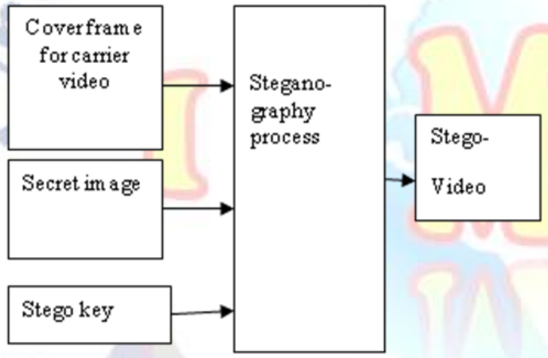


Fig. 1: A sample steganography model for embedding secret image into selected cover frame.

b) Masking and filtering: These techniques are mostly constrained to 24 bits and gray scale image. These techniques generally involve in marking image for hiding information. Embedding procedure involves concealing information in significant areas of cover image.

c) Transformation Techniques: These techniques transform the cover medium to its frequency domain before embedding. Later embedding is performed through modifications of frequency coefficients of cover medium.

II. Related Work

In 2011, Hao et al.[3] proposed a novel video steganography method based on motion vector by using matrix encoding. In this technique to embed the secret data motion vector(mv) having high amplitude is chosen. Into the optimal component (vertical component or horizontal component) of the chosen motion vector, secret data is embedded. This algorithm reduced the modification rate of mv's using matrix encoding technique, as mv's get modified on embedding. The resulted video quality is also high as optimal component is selected for embedding.

In 2012,Kousik Dasgupta et al.[4] proposed hash based least significant bit technique for video steganography. In this paper, a spatial domain technique, LSB is proposed, where hash function is used for selecting the position for inserting secret data bits in LSB bits of cover data. The results has shown minimal degradation of cover video and increased PSNR value and embedding capacity.

In 2012,Rongyue et al. [5] proposed an efficient BCH coding for steganography. In this technique, by changing or modifying various coefficients in the block of cover data, secret data is embedded. This algorithm improves time of computation and embedding capacity. Also reduced the complexity compared to other existing methods.

In 2013,Liu et al.[6] proposed a robust steganography scheme for H.264/AVC video streams.

The algorithm presented mainly focused on preventing intra-frame distortion drift. For improving robustness, secret data is encoded using BCH(n,k,t)syndrome code. For preventing or avoiding intra-frame drift distortion, encoded data is embedded into the coefficients of the luminance I-frame component. The results obtained shown that algorithm can effectively avert intra-frame distortion drift and also achieve high visual quality and robustness.

In 2014,Diop et al [7] proposed new steganography scheme based on Reed Solomon codes and matrix embedding techniques. The algorithm focused on solving bounded syndrome decoding problem raised due to the use of matrix embedding technique in various steganography techniques. The use of Reed-Solomon codes with matrix embedding technique allowed to solve the problem easily.

III. THE PROPOSED STEGANOGRAPHIC TECHNIQUE

A. Frame Conversion

Before embedding, the frame's colour space is converted to an other colour space. Among the existing colour space models YCbCr colour space is chosen. YCbCr colour space removes the correlation between Red, Green and Blue colours.A luminance (Y) part is brightness data, which the human eyes are more sensitive to than the colour parts. As a result, the colour parts (chrominance) can be sub sampled in the video stream and some information will be discarded [8].

B. Discrete Wavelet Transform

DWT method converts the signal from spatial domain to frequency domain. Instead of grouping various frequencies into estimated regions done by other methods like DCT, DWT involves separating frequencies into high, middle and low and also their boundaries form another. The other advantage over Fourier transforms is temporal resolution [9]: both location information and frequency is captured. The process initially considers the cover frame and first level of 2D-DWT image decomposition is applied to it. Then for decomposition process the frame is splitted into four sub-bands using a low pass filter and high pass filter. The four sub bands are:

- LL (approximation)
- LH (horizontal)
- HL (vertical) and HH (diagonal)

Any image's detailed information is contained within the LH, HL, HH sub bands which are middle and high frequencies. LL is a low frequency sub band. It is approximation of the original frame reduced to a quarter of its size [9].Later To the LL sub-bands 2D-DWT is applied. This application creates four new sub-bands. In this algorithm to the hidden data hamming code is applied. Fig.2 illustrates the 2D-DWT.

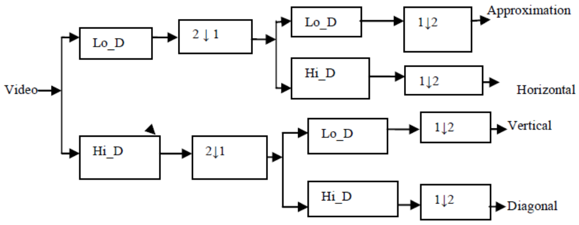


Fig. 2:First level of the 2D-DWT

The results demonstrate the first level of decomposition .Fig.3 shows the second level of the decomposition process.

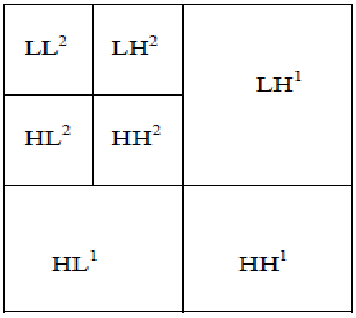


Fig.3: Second Level of the 2D-DWT Decomposition

To achieve a complete reconstruction process, following wavelet reconstruction process, the following wavelet equations must be satisfied:

$[Lo\_D(z)Hi\_D(z)+Lo\_R(z)Hi\_Ri(z)]=2$ (1)

$Hi\_D(z)=z^{-k}Li\_R(-z),Hi\_R(z)=z^{k}Lo\_D(-z)$ (2)

In the above equations, Lo_D(z) and Hi_R(z) represent the wavelet filter bank of the decomposition process. Furthermore, Lo_R(z) and Hi_R(z) signify the wavelet filter bank of the reconstruction process.The following equations are the transfer functions of the Haar wavelet transform filters:

$Lo\_D(z)=1/2(1+z^{-1})$ (3)

$Hi\_D(z)=(z^{-1}-1)$ (4)

$Hi\_R(z)=1/2(z-1)$ (5)

$Lo\_R(z)=(z+1)$ (6)

C. Linear Block Codes:

Linear block codes are concentrated because of their property of linearity and ease of implementation. In short for a linear block code, the XOR of any two valid code words is also a code word. This gives that any code vector can be expressed as a linear combination other code vectors.

Encoding of any message of k bits generates code word vector n of length p bits, resulting from the multiplication of generator matrix G and message vector x.

Because of the property of linearity encoding complexity is reduced greatly. Code rates of linear block codes are very high. Limitation of these codes is that they have limited error correction capabilities.

D. Hamming codes (7,4)

Hamming codes which belong to the family of linear block codes is considered. In general, Hamming codes make use of parity bits. The additional/extra bits added to the binary sequence refer to parity bits. These parity bits allows the binary sequence to have particular parity i.e. either odd parity or even parity and helps in identifying the accuracy of the message.

The specifications for hamming code parameters are as follows, for $p \geq 2$:

- Block length: $m= 2^p - 1$
- Number of message bits: $k = 2^p - p - 1$
- Number of parity symbols: $m - k = p$.

In this paper linear Hamming code (7, 4) is used where 4 message bits are coded into 7 bits by addition of three parity bits. Linear Hamming codes utilize two matrices for encoding and decoding: Generator matrix G, Parity-check matrix H.

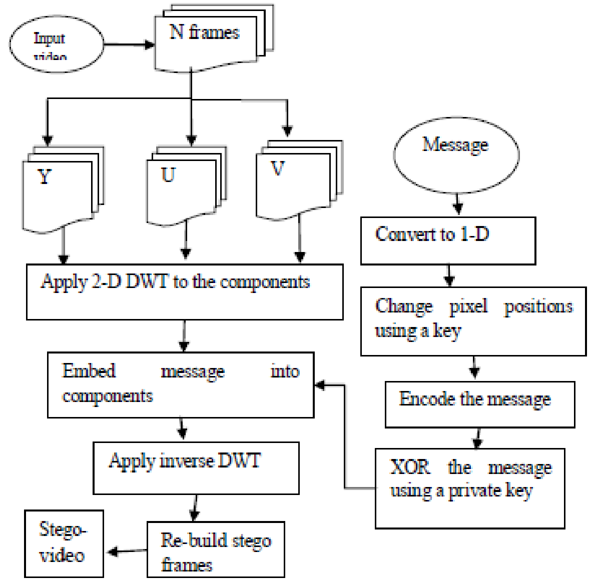
Encoding side: Initially a k-bit message x_1x_2 x_3 x4 is considered as a 1×4 matrix x. Let the generator matrix G be a 4x7, where $G = (P|I_4)$, where P is a 4× 3 matrix, and I, identity matrix of order 4x4. Finally message vector x is encoded as $C=E(x) = xG$, arithmetic modulo 2 is applied over the result of matrix multiplication instead of general summation.

Decoding side: The received vector Y on the decoding side consists of message and parity bits of length m i.e.7. Initially the received vector is checked for error. For checking purpose parity check matrix H is involved. This parity check matrix is the dual code of C, generated by matrix G i.e. $GH^T=0$.So the parity check matrix is $H= [I_{m-k}|P^T]$, where I is an identity matrix of order m-k i.e. 3x3. The checking procedure involves generation of syndrome vector S of 3 bits, where $S=Y \times H^{T}$. If the syndrome vector is of zeroes then the received message is said to be error-free otherwise the received data is erroneous and needs error correction.

E) Data embedding phase:

Data embedding phase is a process of hiding secret message inside host videos. The process involves:

1) Initially the video stream is converted into frames.
2) Selected number of frames are separated into Y, U and V components.
3) To each frame component i.e. for Y, U and V two dimensional DWT is applied separately.
4) The secret message is converted to a one-dimensional array and then the positions of pixels of the whole message are changed by a key.
5) Hamming code (7, 4) is used to encode the message taking 4 bits at a time.


Input video
N frames
Y
U
V
Message
Convert to 1-D
Apply 2-D DWT to the components
Change pixel positions using a key
Embed message into components
Encode the message
Apply inverse DWT
XOR the message using a private key
Stego-video
Re-build stego frames

. **Fig 4: Block Diagram for Data embedding Phase**

6) The result of the encoded data consists of 7 bits (4 bits of message+3 bits of parity) and is XORed with 7 bits of random value using key2.
7) For embedding one of the frequency coefficients LL of Y is chosen and secret message is embedded.
8) After embedding inverse two-dimensional DWT is applied over frame components.
9) Rebuild the stego frames from the YUV stego components.

F) Data extracting phase:

Data extracting phase involves the process of retrieving the secret message from the stego-videos. The process involves following steps:

1) Convert the stego video into frames.
2) Separate each frame into Y, U and V components.
3) Again on each frame components 2D-DWT is applied.
4) Obtain the encoded data from the selected frequency coefficient of YUV components and XOR with the random number using the same key that was used in the receiver side.
5) Decode 4 bits of the message by the Hamming decoder.

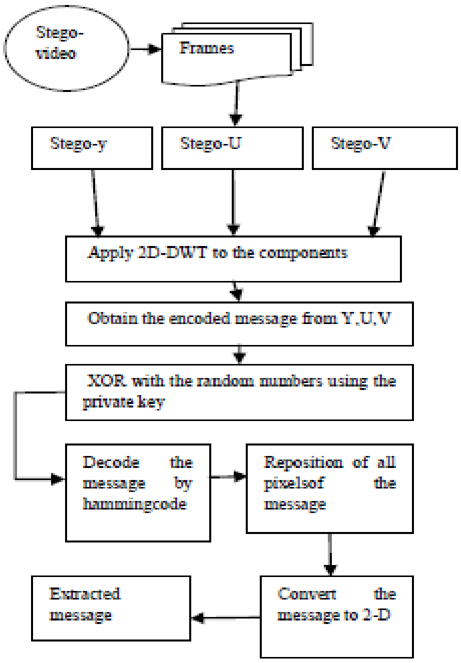

Stego-video
Frames
Stego-y
Stego-U
Stego-V
Apply 2D-DWT to the components
Obtain the encoded message from Y,U,V
XOR with the random numbers using the private key
Decode the message by hammingcode
Reposition of all pixelsof the message
Extracted message
Convert the message to 2-D

Fig 5: Block diagram for data extracting phase

6) Reposition the whole message again into the original order.
7) Convert the message array to 2-D.

IV. RESULTS AND EVALUATION

The simulation is performed on two different video files that act as a cover for encrypted secret data. The properties of test videos are described in table I

Table I: Properties of test videos

Video	Width	Height	Frame rate	No. of frames
Foreman	176	144	25	300
Stationdi	640	360	29	82

A) Outputs:

Due to the difficulty of showing the result as a video stream on paper, original frame, stego frames are displayed along with original message and decoded message.

Fig 6 shows the original message and decoded or retrieved message at the data extraction phase.Fig7 shows the original cover frame before embedding and stego frame.

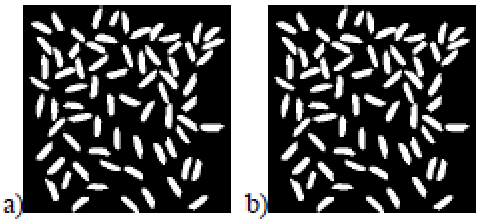


Fig 6: a) Original image b) Extracted image

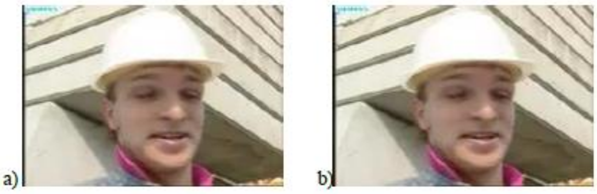


Fig. 7 a) Original frame b) Stego-frame

B) Evaluation and Result Analysis:

- **Visual Quality** This remains the biggest challenge for every steganographic scheme. Achieving this makes the steganographic technique most useful and successful technique. Peak Signal-to-Noise Ratio (PSNR) is the common quality measuring parameter. Original and stego frames differences can be calculated numerically using PSNR.PSNR is generally measured in dB (decibels). It is defined easily through MSE. Higher the values of PSNR, more closely the stego frame to the original frame. PSNR is evaluated using following formula [9]:

$$\mathrm{PSNR}=10*\log_{10}(\mathrm{MAX}^2/\mathrm{MSE}) \quad (7)$$

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[o(i,j)-s(i,j)]^2}{m \cdot n} \quad (8)$$

Where OF and SF denote the original and stego YUV frame components, respectively, and m and n are the number of rows and columns of pixels of frame. Where i and j are indices used to represent a particular row and column respectively. Where, MAX is the maximum possible pixel value of the frame.

Table II: The average psnr values for video sequences

Video sequences	MSE	PSNR
Stationdi	12.895	34
Foreman	14.692	32

From the table it is clear that the obtained PSNR values are greater than 30dB.It indicates that quality of the stego videos are mostly the same as original videos.

- **Processing time:** It is the time required to encrypt and embed the secret message to cover frame. In matlab processing time calculation involves use of tic and toc.

Table III: Processing time values

Video	Processing Time(sec)
Foreman	1.7757
Stationdi	1.6687

III) Security Analysis

The security offered by the technique has been improved and is achieved through usage of 2 keys. These 2 keys are used to make the message unreadable and thus providing safety against attacks. That is even the presence of message is identified, if the keys are not known it is difficult to extract the exact message. Along with the keys, message is encoded using hamming code (7,4) which stands as an extra barrier for attacks.

V. CONCLUSION

In this paper, an enhanced and secured video steganography in the DWT domain based on hamming code has been proposed. Initially the algorithm decomposes video into frames and then each frame is divided into Y, U, and V components. Before the embedding process begins, the secret message is secured by encoding using hamming code. On to each component of the selected frames, 2D-DWT is applied. For embedding the secret data, both the middle and high frequency coefficients of each component are chosen. To provide additional security the algorithm uses two keys during embedding and extraction process. The experimental results have a PSNR value above 30dB.As PSNR value specifies the visual quality of the stego video and from high PSNR value, it is clear that the algorithm has achieved greater visual quality and can be considered to be a high embedding efficiency algorithm as the host data is less modified. The greater visual quality achieved avoids intruder's attention. Furthermore, additionally used keys helps in preventing the message's extraction, even if the attacker gets suspicious about secret message's presence. Also as the message is encoded before embedding, makes the message to be more secured.

REFERENCES

[1]. Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography",2010.

[2]. K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi," LSB Approach for Video Steganography to Embed Images",2014.

[3]. B.Hao ,"Novel video Steganography method based on motion vector by using matrix encoding",2011.

[4]. Kousik Dasgupta, "Hash based least significant bit technique for video steganography", 2012.

[5]. Z.Rongyue,V.Sachney,"An effiecient embedder for BCH coding for steganography:,2012.

[6]. Liu," Robust steganography scheme for H.264/AVC video streams",2013.

[7]. I.Diop ,S.M Farss" New steganography scheme based on Reed Solomon codes",2013.

[8]. https://discoverybiz.net/enu0/faq/faq_YUV_YCbCr_YPbPr.html

[9]. Ramadhan, J.Mstafa, Khaled M.Elleithy,"A high payload video steganography algorithm in DWT domain based on BCH codes(15,11)",2015.