Reversible Video Steganography using Histogram Shifting

Manjunath Kamath K
Assistant Professor, Dept of ISE
Yenepoya Institute of Technology
Moodbidri, India

Dr. R Sanjeev Kunte
Professor, Dept of CSE
J.N.N College of Engineering
Shimoga, India

***Abstract*—In this paper a reversible data hiding (RDH) technique in video which can recover the original video without any distortion from the marked video after the hidden data have been extracted is presented. First the cover video is selected and then by using the key frame extraction algorithm the frame is selected to embed the secret image. Then the algorithm utilizes the zero and the maximum point of the histogram of different channels of a frame and slightly modifies the pixel values to embed data into the image. The peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be above 40 dB.**

Keywords— Reversible Data Hiding (RDH), zero point, maxium point, minimum point.

I. INTRODUCTION

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). Steganography is a data hiding technique that has been widely used in information security applications [1]. It is similar to watermarking and cryptography techniques. Cryptography scrambles the data to be communicated so that unintended receivers cannot perceive the information. However, the fact that the communication has been carried out is known to everyone [2]. Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. The sender hides a message into a cover file likes for e.g. (image, audio, video) and tries to conceal the existence of that message, later the receiver gets this cover file and detects the secret message and receives it.

The process of embedding the data into the cover with a minimum amount of distortion to the original cover is called data hiding. There are two types of data hiding techniques reversible and irreversible. In reversible the original cover can also be recovered, but in irreversible the original cover cannot be recovered.

In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing, medical image sharing, multimedia archive management, image trans-coding and high-energy particle physical experimental investigation, any distortion due to data embedding is intolerable and the availability of the original image is in high demand. The original cover media can be recovered because of the required high-precision nature.

In this paper we have designed a Reversible video stegnography system to hide image in frames of cover video. Secret image is hidden in the random frames found by key frame selection algorithm. Hence, the proposed scheme offers better imperceptibility and increasing capacity and more security over cryptographic approaches.

Rest of the paper is organized as follows. Section 2 briefly introduces previous methods proposed. The proposed work is elaborated in Section 3. Experiments with analysis and comparison are given in Section 4. The paper is concluded in Section 5.

II. RELATED WORK

Hsien *et al.*, [3] propose an algorithm where the lower bound pixels which cause the underflow problems are incremented by 1 and the upper bound pixels which cause the overflow problems are decremented by 1. This method divides the cover image into identical blocks. In each block, a pixel is selected as the base pixel and then the absolute differences between the gray level value of the selected pixel and that of the other pixels. To embed the data the differences are used to generate a histogram and the histogram shifting method is applied. Also propose an offset distortion method which uses the max difference and the min difference to counteract the change in the gray levels of some pixels. The total of the changed gray level values is thus reduced. Therefore, the PSNR value can be increased up to 30 dB and the quality of the stego image improved.

Marin *et.al.*, [4] propose an improved histogram modification reversible data hiding algorithm using multiple scanning techniques. It consists of two stages: encoding the payload within an image to produce the cover image and decoding the cover image to retrieve the payload and the original image. They use three different scanning techniques for the construction of the difference histograms in order to maximize the payload capacity. The scanning techniques used are a horizontal, vertical, and diagonal scanning technique. The scanning order uses adjacent pixels since these are more likely to have similar values and as a result will result in a difference histogram that has most of its values near 0. The technique takes advantage of the fact that the central peaks of the difference value histograms produced by additional scanning techniques are higher than the peaks of increasing the EL of the single horizontal scanning technique. This allows for an image to have more data embedded within it. They have also introduced an algorithm for determining an appropriate scan order and EL.

Xinpeng Zhang *et al.*, [5] propose scheme which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

It is observed from the literature survey, that the majority of the works use complex embedding and extraction algorithm to make the system secure. Also it is found that entire secret image will be embedded in any one selected frame of the cover video.

In the proposed work, simple key frame selection technique is used which increases the security. First the video is divided into frames. By using key selection algorithm, the frames are selected for embedding the data. Then the histogram for the key frame is generated and the maximum-point and the zero-point will be found. The proposed scheme offers better embedding capacity, robust against noise attack than earlier schemes as data is going to embed in the selected key frame.

III. PROPOSED METHOD

The approach presented in this work deals with embedding and extraction of the secret image pixels into a cover video key frame selection method. The cover video considered in this work is an AVI file. This system presents an efficient way of transfer of information from sender to the receiver as data is hidden in the key frames. The frame work for the proposed system is illustrated in the Fig.1.

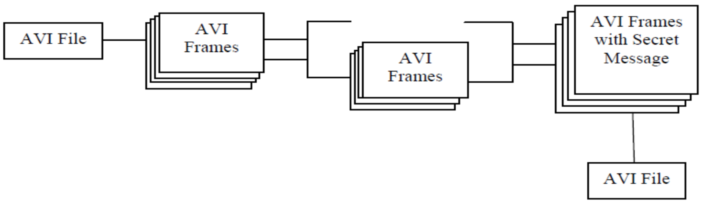


Fig. 1. Framework of the proposed system

The proposed method selects the identical frames as the key frames and then the frame is split into 3 channels, the data are hidden by finding the histogram maximum point and the zero point. The range between the maximum and the zero points are incremented by 1 if the maximum is less than the zero point. The image is scanned once we get the pixel with value equal to maximum point then we check for the data to be embedded bit if it is '0' the pixel value is kept intact otherwise the value will be incremented by 1. The range between the maximum and the zero points are decremented by 1 if the maximum is greater than the zero point. The image is scanned, once we get the pixel with value equal to maximum point then we check for the to be embedded bit if it is '0' the pixel value is kept intact otherwise the value will be decremented by 1. The R, G, B channels are packed back to form the marked image. The process of decoding is opposite to the embedding process.

A. *Embedding Procedure*

- *Embedding Process*

The embedding process consists of various procedures. Initially the host video is converted into frames. After the conversion the key frames are selected. Then the bits are embedded by shifting the histogram. After embedding the frames are converted back to video, which forms the stego video. The Fig. 2 represents the steps in the embedding technique.

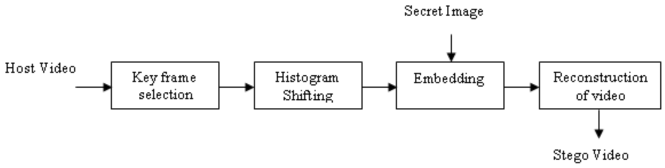


Fig. 2. Process of Embedding

- *Key Frame Selection*

A video is used as a cover medium to hide the information. Video is a set of images which represent the set of actions that are played in a speed of 30 images per second. Here each image is known as frame. In video steganography the secret data are hided in some frames. Key frames are a set of salient images extracted from video sequences. To extract the key frame the following key frame extraction algorithm is used [7] [8].

Data hiding is done on the some of the identical frames. To select the identical frames, the intensity histogram of the frame is compared with the intensity histogram of the adjacent frames.

Step 1: Intensity can be calculated as for RGB frame.

$$I = 0.299R + 0.587G + 0.114B \qquad (1)$$

Where R, G and B represent the Red, Green and Blue channel value of the pixel.

Step 2: The difference in the histogram intensity between adjacent frames can be calculated as

$$D_j = \sum^{N}{}_{j=1}\, h_j - \; h_{j+1} \qquad (2)$$

Where D_J represents the intensity histogram difference, h_j is value of histogram for j_{th} frame and N denotes total number of frames in the video.

Step 3: The identical frames can be found using a threshold value. Threshold value calculated as,

$$T = \mu + \alpha\sigma \qquad (3)$$

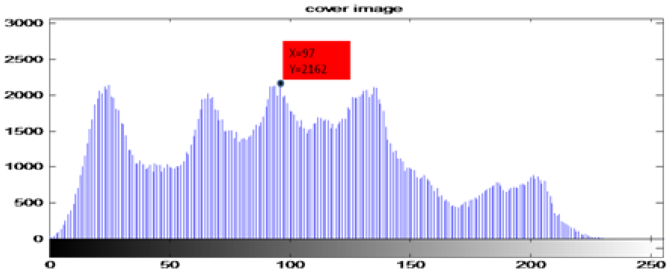
The frames with intensity histogram difference more than T are selected as identical frames. Here µ is mean value and σ is standard deviation of intensity histogram difference. Value of α varies from 2 to 6.

- *Histogram Shifting*

Histogram is nothing but the complex or composite mixture of color representation in a graphical manner. The algorithm uses the zero point and the maximum point of the histogram and modifies the pixel values to embed the data [6]. The algorithm of histogram shifting is described as follows: For a frame of size P*Q, each pixel value x € [0,255].

Step 1: Select the frame from the list of key frames.
Step 2: Generate the histogram H(x) for the red or green or blue channel of the frame. go
Step 3: Find the zero point in the histogram H(x). It corresponds to a value which no pixel the given image holds.
Step 4: Find the maximum point in the histogram H(x). It corresponds to a value which many number of pixel the given image holds.
Step 5: If zero point > maximum point, the value of the pixel between zero point and maximum point is incremented by 1, which results in shifting the histogram towards right leaving a pixel value empty.
Step 6: Otherwise, the value of the pixel between zero point and maximum point is decremented by 1, which results in shifting the histogram towards left leaving a pixel value empty.

Fig. 3 represents the Histogram of cover frame, where maximum point is at x= 97,y=2162, and zero point is at x= 238,y= 0. Fig. 4 represents the shifted histogram. In the figure at the point x=98 the value is left empty. The location of the maximum point and the zero point are sent as the book keeping data.



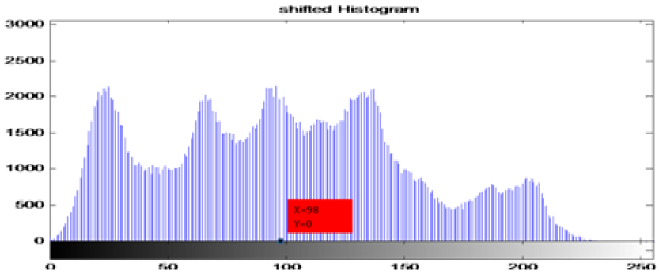


Fig. 3. Histogram of cover image.

Fig. 4. Right Shifted Histogram

- *Embedding*

In this step, the data to be hided are hided using the data embedding algorithm. The data to be hidden is considered as an image. The image is converted into the binary bits format. The algorithm of data embedding is described as follows:

Step 1: The frame is scanned in a sequential order. Find a pixel with a value that is equal to the maximum point.
Step 2: If zero point > maximum point, go to step 3 otherwise to step 5.
Step 3: If the corresponding to-be-embedded bit in the sequence is binary "1," the pixel value is incremented by1.
Step 4: If the corresponding to-be-embedded bit in the sequence is binary "0," the pixel value is kept intact.
Step 5: If the corresponding to-be-embedded bit in the sequence is binary "1," the pixel value is kept intact.
Step 6: If the corresponding to-be-embedded bit in the sequence is binary "0," the pixel value is decremented by 1.

The process of shifting and embedding is done till all the bits of the secret image are embedded. First, in the red channel of the frame the data are hided, followed by the green channel, and the blue channels. The R, G, B channels separated are for embedding are packed back to form the marked frame. If there are still more bits to hide then the next key frame will be selected and the process of shifting and embedding is repeated [9].

- Reconstruction of Video

Once the embedding process is completed, the next step is reconstruction of the video. This is done by replacing the original video frames by the marked frames.

B. *Extraction Procedure*

The extraction process consists of various procedures. Initially the marked video is converted into frames. After the conversion the key frames are extracted. Then the secret age bits are extracted. Then the histogram is shifted back. After the extraction the frames are converted back to video, which forms the host video. The Fig 5 represents the steps in the extraction technique.

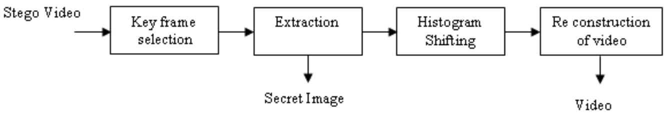


Fig. 5. Process of Extraction

- *Key Frame Selection*

The steps for key frame selection that are explained in embedding are followed and then key frames are extracted.

- *Data Extraction*

In this step, the data hided are extracted using the data extraction algorithm. The algorithm of data extraction is described as follows:

Step 1: The marked frame is scanned in a sequential order. The maximum and the zero point are got by the book keeping data. Find a pixel with a value that is equal to the maximum point.

Step 2: If zero point > maximum point, go to step 3 otherwise go to step 6.

Step 3: If the pixel value is equal to maximum point then ‘0’ is retrieved.

Step 4: If the pixel value is altered i.e. incremented by 1 then ‘1’ is retrieved. And the pixel value will be decremented by 1.

Step 5: The pixels with the values between the maximum point and zero point are decremented by 1.

Step 6: If the pixel value is equal to maximum point then ‘1’ is retrieved.

Step 7: If the pixel value is altered i.e. decremented by 1 then ‘0’ is retrieved. And then pixel value will be incremented by 1.

Step 8: The pixel with the values between the maximum point and zero point are incremented by 1.

If the extracted image bit length is not equal to the secret image bits length, then scan and retrieve the bits from the next key frame till whole secret image bits are got. Thus the marked image is recovered to the original image without any distortion.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed scheme is implemented in MATLAB 10 in the windows environment. Various experiments are carried out by considering cover video and different secret images. The secret image are “*lenna*”, “*peppers*”, “*cameraman*” and “*baboon*”. The size of the secret image is varied and the dimensions considered are 15*15, 25*25 and 35*35.

In the first experiment a single cover video is considered and then the secret image is considered is also same. Experiments are done by varying secret image size. The PSNR and MSE between the original and the stego video are found. The PSNR between the original and retrieved video are also calculated to check for the reversibility.

In the second experiment a single cover video is considered and then the secret image is considered are different. Here the size of the secret image is not altered but the experiment is done by changing the secret images only. Then the PSNR and MSE between the original and the stego video are found.

In the third experiment some noise is included in the stego video and then the secret image is retrieved. Later the PSNR and MSE between the original secret image and the extracted secret image are calculated by altering the percentage of noise.

The performance of the system developed can be analyzed by using the parameters:

- Mean Square Error
- Peak Signal Noise Ratio

The quality of the stego image or the video should be always better such that no intruder can guess the presence of the secret data in it. So the quality of the image can be measured using the MSE.

If I is the size m×n is the original image and K is the stego image then MSE is given by:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j)-K(I,j)]^2 \qquad (4)$$

The PSNR is given by:

$$PSNR = 20\ Log_{10} \left(\frac{MAXf}{\sqrt{MSE}}\right) \qquad (5)$$

Where MAXf is the greatest conceivable pixel estimation of the image. At the point when the pixels are written by utilizing 8 bits for each pixel, this is 255. If there is no difference between the original and the marked media then the MSE will be equal to zero, then the PSNR will be infinity.

Table I gives the MSE and PSNR for lena.jpg for different sizes.

TABLE I. MSE AND PSNR FOR DIFFERENT DIMENSIONS OF SECRET IMAGE

Secret Image	Dimensions	MSE	PSNR (db)
Lena.jpg	35*35	0.0257	64.0584
Lena.jpg	25*25	0.0129	67.0642
Lena.jpg	15*15	0.0048	71.3811

Table II depicts the results considering the different secret image and secret image taken is *baboon, cameraman and the peppers* image and the cover media considered is standard *Rhinos* video. The size of the secret image is 25 * 25.Once again from the results obtained (PSNR >60dB) it can be observed that the system has got good imperceptible property. The performance of the system is analyzed for noise attack. In the cover video *lenna* image of size 25*25 is embedded. Then the stego video is subjected to noise attack by adding noise (salt & pepper) of different level. Then the secret image is extracted and the PSNR and MSE are calculated between the original-secret-image and the extracted secret image.

TABLE II. MSE AND PSNR FOR DIFFERENT DIMENSIONS OF SECRET IMAGE

Secret Image	Noise (%)	MSE	PSNR (db)
Lena.jpg	0.01	2.0703e+003	50.4043
Lena.jpg	0.02	3.7481e+003	47.5768
Lena.jpg	0.03	3.5541e+003	45.6495

Secret Image	Dimensions	MSE	PSNR (db)
Peppers.jpg	25*25	0.0129	67.0584
Baboon.jpg	25*25	0.0129	67.0622
Cameraman.jpg	25*25	0.0129	67.0581

Table III depicts the results for different noise level. It can be observed as the percentage of noise increases the MSE increases and the PSNR decreases.

TABLE III. MSE AND PSNR FOR DIFFERENT DIMENSIONS OF SECRET IMAGE

PSNR between original-secret-image and extracted-secret-image is in between 40 to 50 dB. This shows that the system is robust to noise attack.

From the above results it can be deduced that the proposed scheme offer an improved MSE and PSNR. It is found from experiment the MSE is Zero between the original cover frame and the recovered stego frame. This proves that the system achieves reversibility in data hiding process.

V. CONCLUSION

The methodology explained in this work explores the design and implementation of the reversible data hiding in video steganography. For many of the application the cover media should be recovered as it is after the extraction of the secret-data. The proposed method embeds the secret image in the cover video using histogram shifting method. By using the key-frame-extraction algorithm the identical frames are extracted. The histogram is used to hide the secret image. Since secret-data is randomly embedded the proposed methods provides more security. An encouraging result of more than 60 dB of PSNR of the stego frame v/s the original frame is obtained from the system. In addition, the value of the MSE between the recovered-frame and the original-cover-frame is 0.0 and thus the PSNR is too high, hence the reversibility is achieved.

REFERENCES

[1] C.T Hsu and J.L.Wu, "Multiresolution watermarking for digital images," *IEEE Trans. Circuits Syst. II*, vol. 45, pp. 1097–1101,1998.

[2] Xiaojun Qi and KokSheik Wong, "An Adaptive DCT-Based MOD-4 Steganography Method**",** *In procedings of International conference on ICIP*, Vol 2, pp. 297-300, 2005.

[3] Hsien-Wei Yang, Kuo Feng Hwang and Shou-Shiung Chou, "Interleaving Max-Min Difference Histogram Shifting Data Hiding Method", Journal Of Software, vol. 5, no.6, pp.615-621, 2010.

[4] John Marin and Frank Y. Shih, "Reversible Data Hiding Techniques Using Multiple Scanning Difference Value Histogram Modification", Journal of Information Hiding and Multimedia Signal Processing, vol. 5, no.3, pp. 451-461, 2014.

[5] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", *In Procedings of IEEE Transactions On Information Forensics And Security*, vol.7, no.2, pp. 826-832, 2012.

[6] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, 2006.

[7] Sukhjinder Singh, Neeraj Gill, Gagandeep Kaur "Identical frames based video steganography ", International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, vol. 2, no.7, pp.1729-1732, 2014.

[8] Ganesh. I. Rathod, Dipali. A. Nikam, "An Algorithm for Shot Boundary Detection and Key Frame Extraction Using Histogram Difference", International Journal of Emerging Technology and Advanced Engineering, vol.3, no.8, pp. 155-163,2013.

[9] Sukhjinder Singh, Neeraj Gill, Gagandeep Kaur "Identical Frames Based Video Steganography ", International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, vol. 2, no.7, pp.1729-1732,2014.