IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

A Novel Reserving Room Approach for Reversible Data Hiding Algorithm before Encryption on Digital Videos

G. Akhila[1], P. Rama Krishna[2]

PG Scholar, ECE, Gudlavalleru Engineering College, Vijayawada, India [1]

Assistant Professor, ECE, Gudlavalleru Engineering College, Vijayawada, India [2]

Abstract: In most cases of data hiding, the cover images will experience some distortion due to data hiding and cannot be inverted back to the original form. That is, some permanent distortion has occurred to the cover image even after the hidden data have been extracted out. In a wide range of applications like medical, military and law forensic fields, distortion of cover images does not allowed. So reversible data hiding is essential for these cases. The technique provides the secrecy for a data, and also for its cover image. This paper describes a novel method of reversible data hiding algorithm in which, Reserving room before encryption is done. The proposed method is written in digital videos. In the proposed method the video is converted into different frames and RDH algorithm is applied to each frame. These frames act as media to carry the secret data. The proposed method is free of errors and the payload is increased. PSNR values are also increased. Performance comparisons with other existing schemes are provided to demonstrate the superiority of the proposed scheme.

Keywords: reversible data hiding; encryption; LSB replacement technique; reserving room.

I. INTRODUCTION

Reversible data hiding (RDH) approach in digital images is an innovative technique where the information related to original cover recovered lossless approach; this lossless data extraction is done once the extraction of embedded message is successfully completed. The applications related to reversible data hiding are medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed A researcher named Kalker et al[1] firstly introduced rate distortion model approach for reversible data hiding algorithm which attracts many researchers, since this rate distortion approach proposes a recursive code construction model which yields the data in lossless manner. After some years a researcher named Zhanget at el[2] proposes a novel enhanced rate distortion framework seeing the tremendous importance of reversible data hiding. Reversible data hiding is the technique in which data in the cover image reversibly can retrieve after the extraction of hidden data in it. The technique provides the secrecy for a data, and also for its cover image. Ancestor methods of reversible data hiding were vacates room for data hiding after encryption, which leads to some errors at the time of data extraction and image recovery. This method describes a novel method of reversible data hiding in which, Reserving room before encryption in images, so that image extraction is subjected to free of errors.

II. RELATED WORK

In Jui Tian has introduced a difference expansion technique which discovers extra storage space by exploring the redundancy in the image content[3]. . Both the secret data holding capacity limit and the visual quality of embedded images of the DE method are among the best in the literature, along with a low computational complexity.

Wen-Chung Kuo, Po-Yu Lai, Lih-Chyau Wuu has proposed a new method of adaptive reversible data hiding based on histogram. In order to enhance the data hiding capacity and embedding point adaptively anew proposed scheme was based on histogram and slope method. This method keeps the embedding capacity high and also maintains the high quality of stegno-image[8] .

Kede Ma, Weiming Zhang,has proposed a framework for reversible data hiding for embedding data in an image by reserving room before encryption. Since losslessly vacating room from the encrypted images is relatively difficult and sometimes in efficient[9]

Kuo-Ming, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen has proposed method that combines reversible data hiding, halftoning and vector quantization (VQ) technique[4] to embed a grayscale image in other image. In embedding, first use halftoning to compress the image from grayscale to halftone. Next, compute th difference between original image and one which inversed by LIH. Employing the VQ compress the difference and embed it with secret data. Then the host image can be recovered better when extracting the secret data by the difference. In the area of reversible data hiding José .R; Abraham .G, in have proposed a novel scheme to reversibly hide data into encrypted greyscale image in a separable manner.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

III. PROPOSED METHODOLOGY

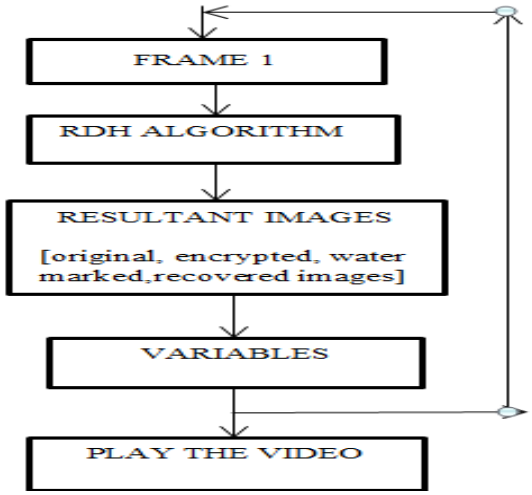


Fig.1. Flow chart of RDH algorithm reserving room before encryption on digital videos

The flow chart shown in Fig1 explains the procedure to implement the reversible data hiding reserving room before encryption on digital videos. First the video is converted into frames and to each frame the RDH algorithm is applied and the resultant images i.e., original image, encrypted image, water marked image and recovered images are stored in different variables and finally when we play all the variables we get the respective videos.

PROPOSED METHOD BLOCK DIAGRAM

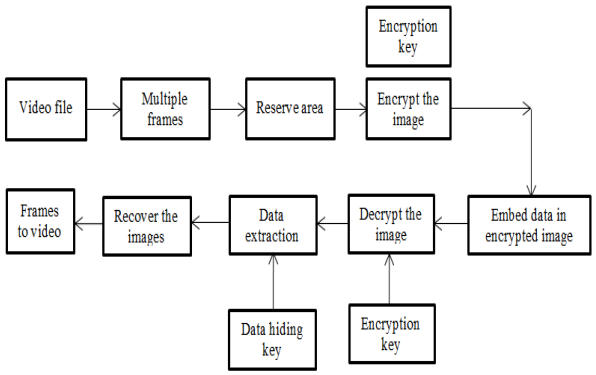


Fig.2.block diagram of proposed method

A. Generation of encrypted frame:

Actually, to construct the encrypted image, the first stage can be divided into three steps: image partition, self reversible embedding followed by image encryption.

(a)Frame partition

At the beginning, image partition step divides original image into two parts A and B; then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition is to construct a smoother area B, on which standard RDH algorithms such as [8], [9] can achieve better performance. To do that, assume the original image C is an 8 bits gray-scale image with its size M×N and pixels $C_{i,j} \in [0,255]$, $1 \le i \le M$, $1 \le j \le N$. First, the content owner extracts from the original image C, along the rows, several overlapping blocks whose number is determined by the size of embedded messages. In detail, every block consists of m rows, where m= [1/n], and the number of blocks can be computed through n=M-m+1.. For each block, define a function to measure its first-order smoothness

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \right| \quad (1)$$

Higher f relates to blocks which contain relatively more complex textures. The content owner, therefore, selects the particular block with the highest f to be A, and puts it to the front of the image concatenated by the rest part with fewer textured areas, as shown in Fig. 3.

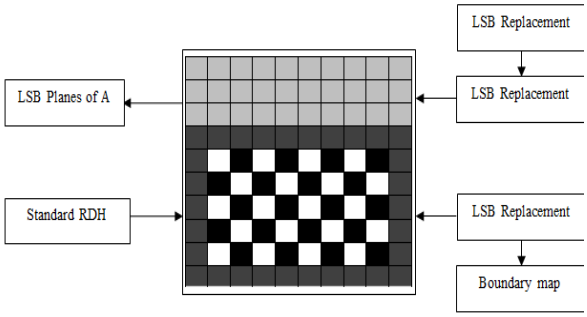


Fig.3.Partition and embedding process

(b) Self Reversible Embedding

The goal of self-reversible embedding is to embed the LSB-planes of A into B by employing traditional RDH algorithms. For illustration, we simplify the method in [10] to demonstrate the process of self-embedding. Note that this step does not rely on any specific RDH algorithm. Pixels in the rest of image B are first categorized into two sets: white pixels with its indices i and j satisfying (i+j) mod2=0 and black pixels whose indices meet (i+j) mod2=1, as shown in Fig. 2. Then, each white pixel B_{ij}, is estimated by the interpolation value obtained with the four black pixels surrounding it as follows

$$B'_{i,j} = w_1 B_{i-1,j} + w_2 B_{i+1,j} + w_3 B_{i,j-1} + w_3 B_{i,j+1} \quad (2)$$

Where the weight w= $1 \le i \le 4$, is determined by the same method as proposed in [1]. The estimating error is calculated via $e_{ij}=B_{ij}-B'_{ij}$.

(c) Frame Encryption

After rearranged self-embedded image, denoted by X, is generated, we can encrypt X to construct the encrypted

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

image, denoted by E. With a stream cipher, the encryption version of X is easily obtained. For example, a gray value $X_{i,j}$ ranging from 0 to 255 can be represented by 8bits, , such that $X_{i,j}(0)$, $X_{i,j}(1)$, $X_{i,j}(2)$…….. $X_{i,j}(7)$

$$X_{i,j}(k) = \left\lfloor \frac{X_{i,j}}{2^k} \right\rfloor \bmod 2, \qquad k = 0, 1, \dots, 7 \qquad (3)$$

The encrypted bits $E_{i,j}(k)$ can be calculated through exclusive-or operation

$$E_{i,j}(k) = X_{i,j}(k) \oplus r_{i,j}(k) \qquad (4)$$

Where $r_{ij}(k)$ is generated via a standard stream cipher determined by the encryption key. Finally, we embed 10 bits information into LSBs of first 10 pixels in encrypted version of A to tell data hider the number of rows and the number of bit-planes he can embed information into. Note that after image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

B. Data Hiding in Encrypted Frames

Once the data hider acquires the encrypted image E, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of A, denoted by A_E. Since A_E has been rearranged to the top of E, it is effortless for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of `pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data m. Finally, the data hider sets a label following m to point out the end position of embedding process and further encrypts m according to the data hiding key to formulate marked encrypted image denoted by E'. Anyone who does not possess the data hiding key could not extract the additional data.

C. Data encryption and frame recovery

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.

1) Case 1: Extracting Data from Encrypted Images: To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of our work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

2) Case 2: Extracting Data from Decrypted Images: In Case 1, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed.

D. Generating the marked Decrypted Frame

Step 1: With the encryption key, the content owner decrypts the image except the LSB-planes of A_E. The decrypted version of E' containing the embedded data can be calculated by

$$X''_{i,j}(k) = E'_{i,j}(k) \oplus r_{i,j}(k)$$

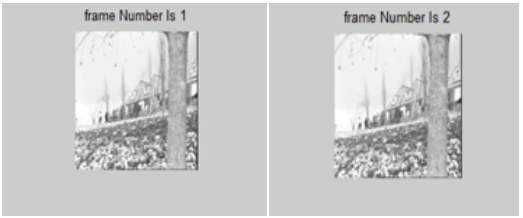
$$X''_{i,j} = \sum_{k=0}^{7} X''_{i,j}(k) \times 2^k \qquad (6)$$

Step 2: Extract the SR and ER in marginal area of B' The plain image containing embedded data is obtained.

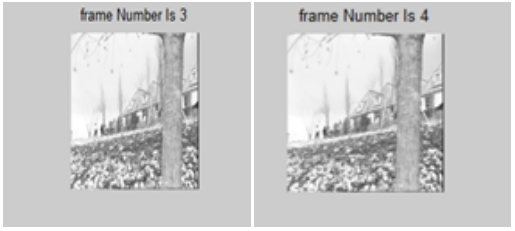
IV. EXPERIMENTAL RESULTS

A.MULTIPLE FRAMES

Frame number 1 Frame number 2



Frame number 3 Frame number 4



B.ENCRYPTED FRAMES

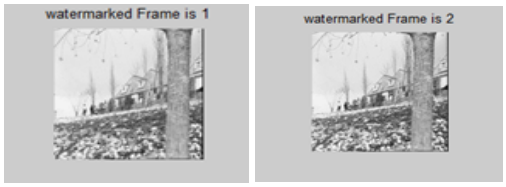
Encrypted frame 1 Encrypted frame 2

Encrypted frame 3 Encrypted frame 4

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

C.WATERMARKED FRAMES

Watermarked frame1 Watermarked frame 2



Watermarked frame 3 Watermarked frame 4

D.RECOVERED FRAMES

Recovered frame1 Recovered frame 2

Recovered frame3 Recovered frame 4

E.ORIGINALVIDEO F.ENCRYPTEDVIDEO

G.WATERMARKED VIDEO H.RECOVERED VIDEO

V. PSNR VALUES

To compute the PSNR, the block first calculates the mean-squared error using the following equation

$$MSE = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M*N}$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. The PSNR value is calculated by using the following equation

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

In the previous equation, R is the maximum fluctuation in the input image data type. The PSNR values are compared with the existing method i.e reversible data hiding using histogram modification on videos and the proposed method gives better PSNR value as shown in table

COMPARISON:

S NO	VIDEO NAME	FRAME NO	EXISTING METHOD PSNR (DB)	PROPOSED METHOD PSNR (DB)
1	Original.avi	**1**	26.5593	37.2896
		4	26.4388	37.0998
		6	25.5723	37.6899
2	Traffic.avi	**2**	31.9676	41.5055
		4	31.4370	43.8325
		6	28.9202	44.5990
3	Car.avi	**1**	34.0321	44.1732
		5	32.7171	44.4576
		7	29.2391	44.5127

VI. CONCLUSION

The reserving room approach for reversible data hiding algorithm before encryption on digital videos is implemented, payload is increased and errors are minimized. PSNR value is also increased and it is compared with the existing method.

REFERENCES

[1] IEEE transactions on information forensics and security, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li vol 8.no 3, march 2013.
[2] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012
[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans.Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[4] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec.2011.
[5] L. Luo et al., "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[6] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang,"Reversible Data Hiding Based on Histogram Modification of pixel differences" ieee transactions on circuits and systems for video technology, vol. 19, no. 6, june 2009
[7] 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.
[8] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
[9] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEETrans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.