Proposed Method for Video Watermarking

Ahmed Y. Yousif

Abstract

Nowadays, daily communications of all kinds over the Internet have become incredibly popular. However, message transmissions over the Internet still have to face all kinds of security problems. While aim of cryptography is protecting the content of messages, steganography is the technique for hiding additional information in cover data. In this paper an embedding method in video is proposed, in which the embedded data is reconstructed without knowing the original host video or any other information about the embedding process. The proposed method enables high rate of data embedding and is robust to compression method since it works in the DCT domain.

Embedding is based on AMELSBR method for compute embedded capacity per block per frame and the DCT coefficient parameter for embedding process. The selection of frame for embedding is done randomly also selection of block for actual embedding is done randomly to increase complexity and security , the embedded data was repeated before hiding in order to ensure robust extraction and reconstruction under any consideration.

1. Introduction

The internet and the World Wide Web have revolutionalized the way in which digital data is distributed. The widespread and easy access to multimedia content has motivated development of technologies for digital steganography or data hiding, with emphasis on access control, authentication, and copyright protection. Steganography deals with information hiding, as opposed to encryption. Much of the recent work in data hiding is about copyright protection of multimedia data. This is also referred to as digital watermarking. Digital watermarking for copyright protection typically require very few bits, of the order of 1% or less of the host data size. These watermarks could be alpha-numeric characters, or could be multimedia data as well. One of the main objectives of this watermarking is to be able to identify the rightful owners by authenticating the watermarks [1]. As such, it is desirable that the methods of embedding and extracting digital watermarks are resistant to typical signal processing operations, such as compression, and intentional attacks to remove the watermarks [2]. In this paper, a watermark method will embed copyright message in a video and

create a new cover. The new cover video is produced using the proposed method for embedding.

2. Minimum-Error LSB Replacement Method (MELSBR)[3]

In gray scale image, there are total 256 levels to represent the intensity of each pixel. If we were to embed k (k<8) bits of message in a pixel, directly replacing the k-LSBs of the pixel will introduce less error than replacing any other k-bits, and the maximum error is 2^k -1.
In the total 256 gray levels, there are $2^{(8-k)}$ gray levels with the same value in the k least significant bite as the k message bits. To reduce the embedding error, we should select the one that has minimum-error with the original gray level to replace the pixel level. To reach the aim, a simple way is provided. It will adjust $(k+l)^{th}$ LSB, and check it's embedding error. And then select the gray-scale with less embedding error to replace the original ones. Figure (1) illustrates the adjusting method, which contains two steps and is called minimum-error LSB replacement method (MELSBR). Using the MELSBR method, the maximum error can be restricted to $2^{(k-1)}$.

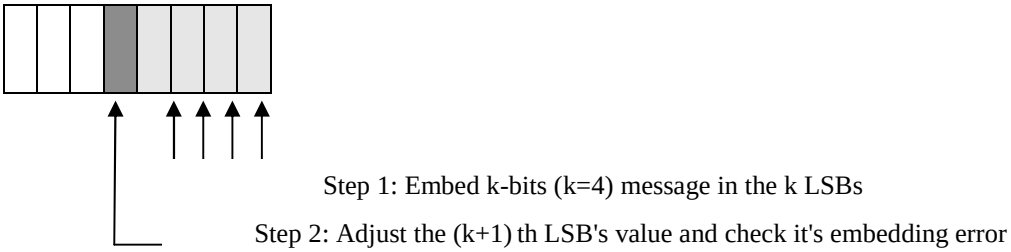


Figure (1) Two Steps of MELSBR method

3. Adaptive MELSBR Method [3]

This method works by tacking advantage of local characteristics of cover image base on the MELSBR.

The upper bound (U) of embedding capacity for each pixel in the cover image is evaluated,

$$U = \lfloor \log_2 (X) - 1 \rfloor \quad (1)$$

where X is the gray level of pixel x, the embedding capacity K of pixel x is defined as the minimum number of bits to store the value D minus 1,

$$K = \lfloor \log_2 (D) \rfloor \quad (2)$$

D for each pixel is equal to the difference between the maximum and minimum gray level of pixel x neighborhood as shown in Figure (2).

$$D = \max \{a, b, c, d\} - \min \{a, b, c, d\} \quad (3)$$

a	**b**	**c**
d	**x**	

Figure (2) the mask for evaluating the Gray variation in the neighbours of pixel "x"

The number of bits pixel can embed k* = minimum (U,K).

Finally, to avoid embedding message in local area a scatting method is provided. To scatter a message a random number with value in [0,1] is generated for each pixel to decide weather the pixel is used to embed Message bits by compare its value against P , where P = AM/ C , embedding ratio, amount of message, predictive embedding capacity respectively.

4. The Proposed Watermark Method in Video

The proposed method used to embed a watermark in video. The watermark is a text data. This method of watermark classified as private watermark that does not need the original data but need the watermark to extract data and compare them and this facility made it suitable to use in copyright protection and authentication services. Figure (3) give the general framework for the proposed system.

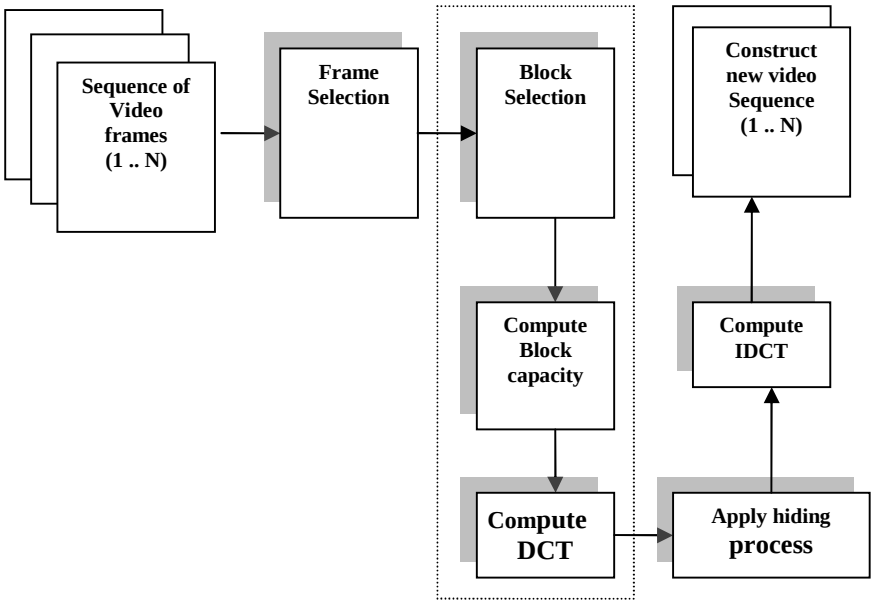


Figure (3) general framework for the proposed method

Before select frame the number of video frames (N) factored using any factorization algorithm, in this paper Fermat factorization is used to produce two distinct number X and Y which represent the dimension of two dimension matrix then this matrix filled with integer number in the range $1 \leq z \leq N$.

Frame selection: to select frame from the matrix an index consist of i and j (i represent row and j represent column) must be prepared. This index can be computed by using the hash value for the number of frame (N). The resulted 160bit digest using SHA-1 algorithm is used to provide index each time a frame must be selected. The index is computed frequently by get binary string of bits from the hash value with length (binary(X) +binary(Y)) then spilt it into two parts one for each index, convert it into decimal then retrieve frame number at that position. Further sub process was take account in the case of repeated index or if the length of digest not enough to complete hiding process. Figure (4) shows this process in details.

Block selection: this process take place after the frame selection, when the frame is retrieved it divided into blocks each of length 8×8 pixels per block, for any frame used in this paper the frame size is 256×256 and the number of block is 32×32 block each.

The index of block selected depend in the index of selected frame, I and j are converted into binary, concatenated to form binary string, then the string reordered to form new string, finally the new string converted into decimal value represent the block index relative to the current selected frame. Figure (5) illustrate the complete computation process.

Compute block capacity: block capacity is computed using equation (1) and (2) illustrated above in section. The selected block consider x and its neighborhood treated as a, b, c, d. if the

value of any parameter(x, a, b, c, d) is grater than 256 then it's reduced by dived it by 256.

Embedding process: the selected block is converted into DCT domain, and then the embedding process is done by manipulating the DCT coefficient, the encoding process is implemented along one diagonal direction forward or backward depend in the frame number retrieved. If frame number is even then encoding is done in forward direction, backward otherwise. If the diagonal start at position(0,0) and end at (7,7) since block size is 8 ×8 then the coefficient around these positions are used in encoding process as follow, if the selected block denoted as b_k, the current position to be used is $b_k(i,j)$ then the surround coefficient laid in the position $b_k(i,j+1)$ and $b_k(j+1,i)$. embedding condition simply denoted as if $b_k(i,j+1) > b_k(j+1,i)$ then the encoding bit is "1" otherwise the encoding bit is "0". Figure (6) illustrated forward and backward direction of embedding.

If the condition not satisfy at any case swap operation used. Finally, minimum bits block can embed are 1 and maximum bits are 7. After the embedding process is completed IDCT process is applied to the modified block.

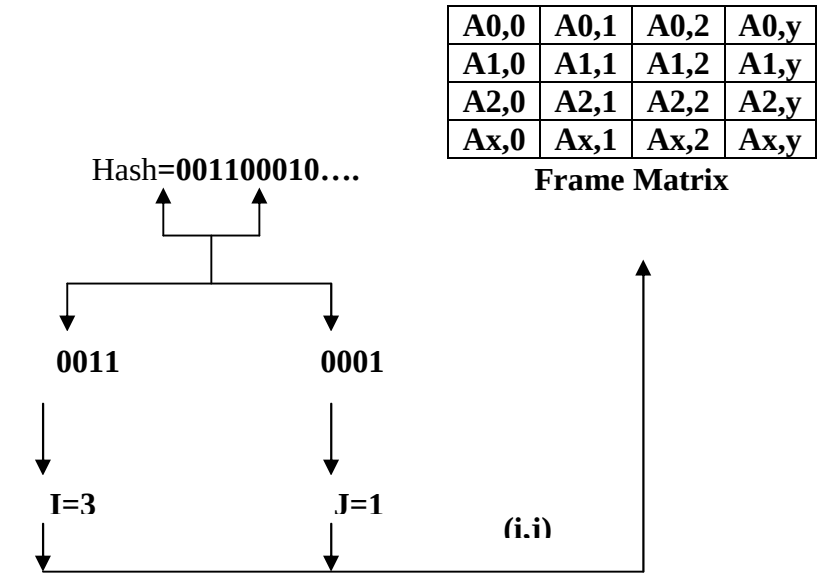


Figure (4) Frame selection process

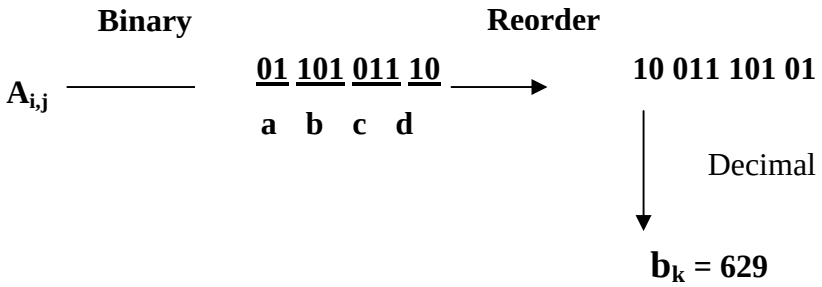
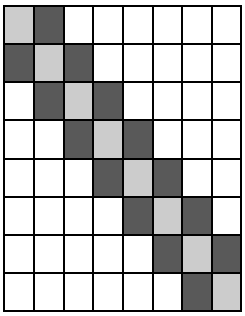
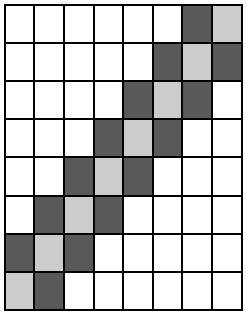


Figure (5) block selection process



a. forward direction



b. backward direction

Figure (6) embedding process in DCT coefficient

5. Embedding Algorithm

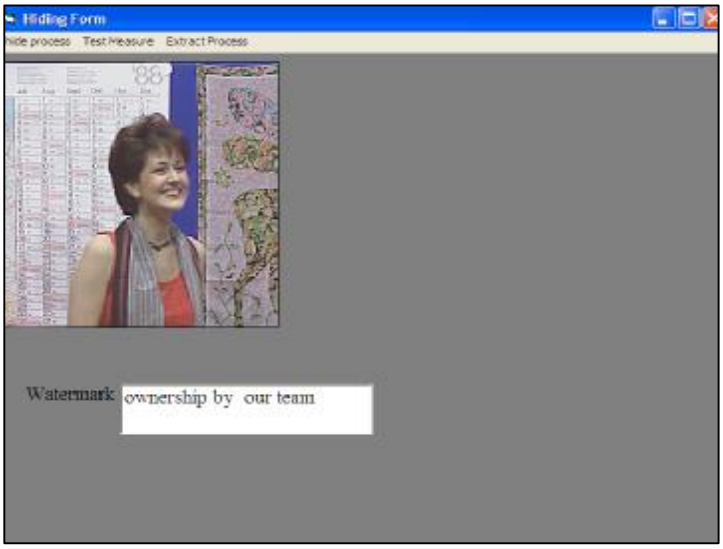
1. ***Convert video into image sequence from 1 to N.***
2. ***Factor N to get matrix of frame dimension X any Y.***
3. ***Fill the frame matrix with integer number from 1 to N.***
4. ***Compute hash value for N.***
5. ***repeat step 6 to 13 while the embed data not empty***
6. ***compute index based on hash value index(I,j)***
7. ***Retrieve frame number from matrix of frame at index (I,j).***
8. ***Partition frame into block of size 8×8 pixel.***
9. ***Generate block index based on frame number then select block for hiding.***
10. ***Compute block capacity using eq( ) and eq( ).***
11. ***Convert block into DCT domain.***
12. ***Apply hiding process forward or backward based on frame number.***
13. ***Apply IDCT to the modified block.***
14. **Go to step 6 while not empty of embed data.**
15. **End.**

6. Extraction algorithm

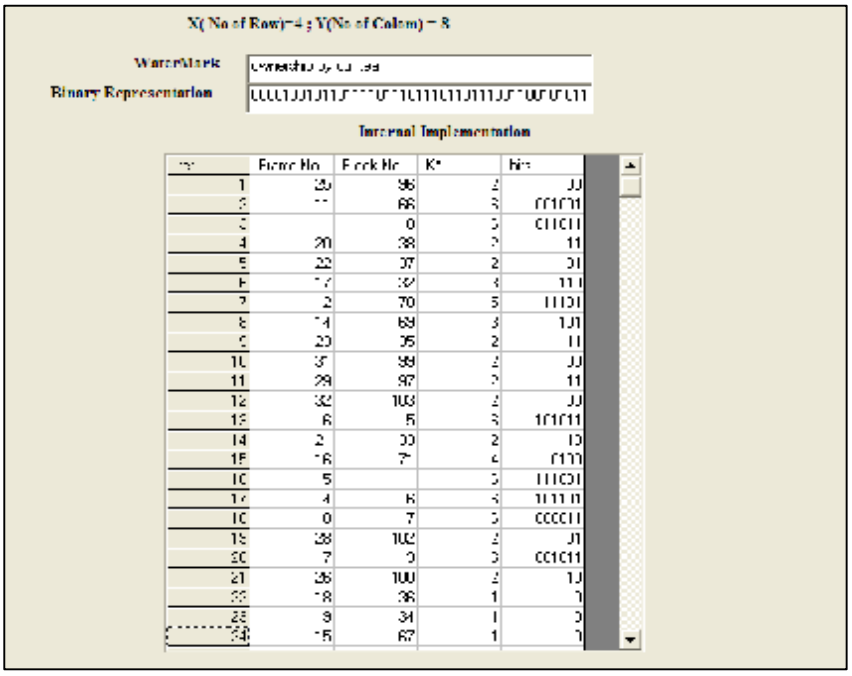
The same sequence of steps in embedding algorithm performed with some changes in step 12 perform extraction process rather than hiding , step 13 not necessary to implement, finally the process is continue while the hide data not completely reconstructed.

7. Experimental Result

A test was made to the proposed watermark algorithm, using selected video cover "renata" and a watermark " ownership by our team", figure(7) shows the input form for the program, figure(8) shows the details of implement the algorithm, figure (9) illustrates the first 6 frame used in the watermarking and their index.

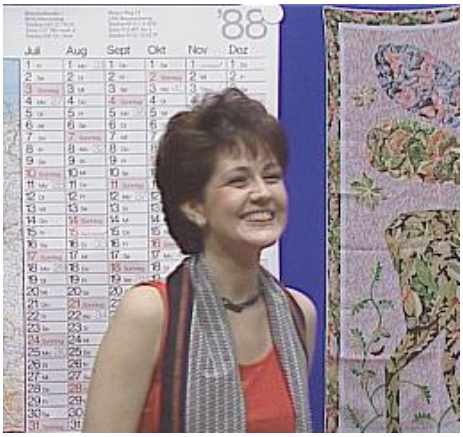


Figure(7)selected video cover and watermark



Figure(8)internal implementation of the proposed algorithm

Frame#25,blockNo=96,K*=2,bits=00



Frame#11,blockNo=66,K*=6, bits=001001

Frame#1,blockNo=0,K*=6,bits=011011

Frame#20,blockNo=38,K*=2,bits=11

Frame#22,blockNo=37,K*=2,bits=01 **Frame#17,blockNo=32,K*=3, bits=110**

Figure (9) the first 6 frame after embedding

9. Conclusion

In this paper a watermark in video method was proposed, this method based on AMELSBR to compute capacity for hiding in each frame method and DCT domain coefficient for hiding, frame selection method is randomly done and each frame is divided into 32×32 block each of size 8× 8 pixels, hiding process is done by manipulating the DCT coefficient diagonally along one direction forward or backward depend on the frame number.

References

1- **J. J. Chae and B. S. Manjunath,"**Data Hiding in Video", **Department of Electrical and Computer Engineering,University of California, Santa Barbara.**

2- **Joshua Silman, 2001 "Steganography and Steganalysis: An Overview", http://www.sans.org/reading.room**

3- **Stefan K. Enbcisser and Fabien A. Petitcolas, 2000 , "Information Hiding Techniques for Steganography and Digital Watermarking", Artech house Inc,USA.**

4- **Yeuan-Kuen L. & Ling-Hwei C., 1999, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement". http://debut.cis.nctu.edu.tw/Publications/pdfs/C14.pdf**

طريقة مقترحة للعلامة المائية في متسلسلة الصور

احمد يونس يوسف

المستخلص

ي ف الوقت الحاضر، جميع انواع الاتصالات اليومية عبر الانترنت اصبحت شائعة بالرغم من ذلك ارسال الرسائل عبر الانترنت لا يزال يواجه المشاكل الامنية، طالما ان الهدف من التجفير هو حماية الرسائل فان اخفاء البيانات هي تقنيةاخفاء معلومات اضافية . في هذا البحث تم اقتراح طريقة للاخفاء في متسلسلة الصور بحيث ان البيانات المخفية يتم استرجاعها دون الحاجة الى الغطاء الاصلي.الطريقة لمقترحة توفر امكانية خزن نسبة بيانات عالية وهي تقاوم طرق الضغط طالما انها تعمل في DCT . الاخفاء يعتمد على طريقة AMELSBR في احتساب سعة الكتلة الواحدة في كل صورة من المتسلسلة في الاخفاء وعلى معاملات DCT في الاخفاء الفعلي للبيانات. اختيار الصورة من المتسلسلة في الاخفاء يكون عشوائي وكذلك اختيار الكتلة ضمن هذه الصورة يكون عشوائي لزيادة التعقيد والعشوائية. البيانات المخفية يتم تكرارها قبل عملية اخفاءها لتسهيل عملية اكتشافها تحت اي ظرف.

Keyword: steganography,AMELSBR,DCT,watermark