

A New Data Embedding Method into Motion Pictures

Ozcerit,A.T.

Computer Science Department
University of Sakarya
Sakarya, TURKIYE
aozcerit@sakarya.edu.tr

Cetin,O.

Computer Science Department
University of Sakarya
Sakarya, TURKIYE
ocetin@sakarya.edu.tr

Cakiroglu,M.

Computer Science Department
University of Sakarya
Sakarya, TURKIYE
muratc@sakarya.edu.tr

Abstract - *In this paper, we introduce three methods bringing new solutions to the communication security which is of great importance in modern communication systems. The methods proposed include data embedding and a new R-weighted coding scheme enabling more data to be stored in video streams. In the first proposal, an RGB-weighted mean value technique is used to obtain a reduced frame to store data. In the second one though, the wavelength, a property of the visible light, is utilized as a parameter for embedding data. Both methods can be used as a source for R-weighted coding technique, which is used for data embedding as a final step.*

Keywords: Steganography, Data Hiding, MPEG, Data Embedding.

1 Introduction

With the increasing importance of the security in communication systems, many research topics have been focused on data embedding into digital media [1-2-3-4-5-6-7-8]. In this paper, it is aimed to develop three methods in which data is embedded into MPEG (Moving Pictures Expert Group) media. Enabling to embed large amount of data and processing the data easily are some advantages of the digital videos. The simplest way to create a moving picture is to playback 25 frames per second consecutively at minimum. In this manner, the human eyes perceive the motion pictures as a movie. Conversely, the human eyes find difficulties to perceive the motion pictures less than 25 frames per second because of the biological properties of the eyes. The motion picture frame numbers are preferred by using those properties of the human eyes [9]. The proposed methods are to embed data into video streams rather than to embed data into pictures [10]. In the second section, we describe basic stenographic methods and digital video basics followed by defining the proposed methods. The discussion part takes place in the third section, discussing alternative methods and in the last section the proposed methods are evaluated and advantages and disadvantages are presented.

2 Data Embedding Techniques

2.1 Digital Video

Images are made up with pixels, the smallest part of the image, which can be accepted as foundation stones of pictures. A pixel (for color images) is combined from Red, Green, and Blue colors. Other intermediate colors are created from the mixture of basic colors in specified proportions. In 24-bit color form, every color is represented by 8-bits, that is, their value is ranging from 0 to 255, so that a pixel is represented by 24-bits in total. Such arrangement can create 224 (apx. 16.7M) colors in many contrasts [10].

A VCD (Video-CD) frame is composed of 352x240 pixels with 24-bit color depth. Thus, the total capacity for a frame is $352 \times 240 \times 3 = 253,440$ bytes. For a 10-second movie at 25 frames/sec will yield $253,440 \times 25 \times 10 = 58\text{MB}$.

Using the previous computation, a 70-minute VCD movie can be as large as 24.36GB which is mostly inconvenient capacity for all applications nowadays. The problem even gets worse in the case of real-time data transfer of the VCD media, which must be 50.688MBit/s minimum. The speed rate is practically unfeasible for most Internet users and companies.

These problems can be overcome by compression techniques. Although the video quality affected by such techniques, the feasibility of the video transfer and media storing could be realized. MPEG is a very common video compression standard, accommodates some versions such as MPEG-1, MPEG-2, and MPEG-4.

2.2 Stenography

In steganography, the data is first embedded into innocent carriers and then sent or ported to the destination. The techniques and methods used throughout this procedure are called stenographic methods or techniques. The carriers can be picture, video, text or other digital media files [11].

Today, the Internet is widely and effectively used in many areas and it has become one of the crucial medium to communicate between people and machines. However, its security infrastructure is not sufficient enough in some applications. The security measures have been deployed as they needed, however in some cases, this combines a trial-error design process and the security measures can not guarantee absolute solutions.

Solution mostly comes with cryptographic methods and algorithms. However, the cipher text can be readily noticed by third parts and it can find itself under massive attack to reveal its secret. In the case of hiding communication purposes, the data masking techniques are also deployed. The masking techniques can be seen as a stenographic approach in which the communication data is converted to a form and virtually impossible to be noticed as suspicious data. There are many methods developed by many researchers [12, 13, 14] to hide information within pictures. For example, Least Significant Bit (LSB), adding noise, image processing, compression algorithms, and luminance properties modification are amongst them.

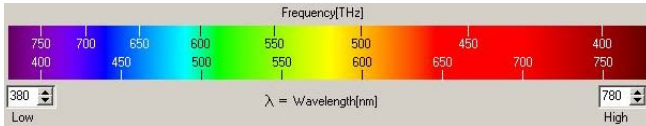


Figure 1: Linear wavelength values [nm] are shown along the bottom edge; non-linear frequency values [THz] are shown along the top edge.

2.3 The Visible Light

The wavelengths of a pixel can be utilized as data storing object by determining appropriate segments. As seen in Figure 1, each color has individual wavelength and frequency values. We can detect only a very small segment of this spectrum directly through our sense of sight. This range is called visible light and the wavelengths range from about 400 to 740 nm ($400 \text{ to } 740 \times 10^{-9} \text{ m}$), with corresponding frequencies from about 750 to 430 THz ($7.5 \text{ to } 4.3 \times 10^{14} \text{ Hz}$). Wavelengths for colors in the visible spectrum are given (very approximately) in Table 1.

Table 1: Wavelengths of Visible light

Wavelength range (10^{-9} m)	Color
400 to 440	Violet
440 to 480	Blue
480 to 560	Green
560 to 590	Yellow
590 to 630	Orange
630 to 740	Red

2.4 Proposed Methods

Many studies have been done recently on information hiding within digital media, which is also called watermarking [15, 16, 17, 18, 19]. However, most of them have focused on spatial domain of data hiding, such as motionless image or picture. A few studies demonstrate temporal domain as well as spatial domain [20-21]. In this paper, we proposed two methods comprising both of domains to hide information within the digital video.

We first have maintained each frame from the video stream. The frames are used as a target storing media to hide the data. The maintained frames have been reduced by using least common multiple method in order to obtain appropriate pixel sets for data hiding. The ASCII codes have been inserted into the new pixel maps by means of R-weighted coding technique and a method specifying data hiding algorithm.

2.4.1 RGB-weighted Segmentation

Digital movies are made up digital pictures which are called as frames. In our approach, the frames are obtained from the digital movie by using sampling method. The frames are segmented and, therefore, segments of the frames are obtained. For instance, a 352×240 pixel Video-CD movie frame is obtained as 16×16 pixel segment. Thus, a new frame is created as 22×15 pixel arrays. In the second step, every segment is compared with their RGB-weight values by the help of arithmetic mean. Every segment is tested whether it is in the determined boundaries. The segment is labeled as logic 1 in determined boundaries and labeled as logic 0 in otherwise cases. By the help of these logic values, appropriate regions are located to hide data.

The regions located as logic 0 are defined as “critical regions” in which the color changes are significant. It means that the color change in this area is realized at extreme ends. Therefore, they are not feasible areas for data hiding. By segmentation of each frame in this manner, tracing of inter-frame changes are maintained easily. Additionally, potential pixel faults caused by undesired pixel changes, which can be originated by transmission media, can be avoided. In the final step, the ASCII codes are embedded into the areas where their logic is “1” by the method of R-weighted coding. There may no crucial data corruption in the final bit stream and a large rate of data capacity can be attained by this method i.e. 1-pixel/1-byte. On destination, the perceptibility of the changes in the video stream is extremely difficult since only a fraction of the frame bits are processed.

An example is given below to elucidate the processes mentioned above. In Figure-2, a 10×10 pixel frame is selected and the frame is divided into as 2×2 pixels. The RGB values of each pixel belonging to marked area are shown at the right-hand side. The RGB-weighted arithmetic mean of values can be calculated by Equation 1, 2, and 3.

$$\text{R-weighted arithmetic mean} = \sum_{i=1}^{i=4} \left(\frac{R_i}{4} \right) \quad (1)$$

$$\text{G-weighted arithmetic mean} = \sum_{i=1}^{i=4} \left(\frac{G_i}{4} \right) \quad (2)$$

$$\text{B-weighted arithmetic mean} = \sum_{i=1}^{i=4} \left(\frac{B_i}{4} \right) \quad (3)$$

The frame, which includes segments consisting of 4 pixels, is reduced into a 5x5 pixel array by the help of calculation in Equation 1, 2, and 3 as shown in Figure-2.

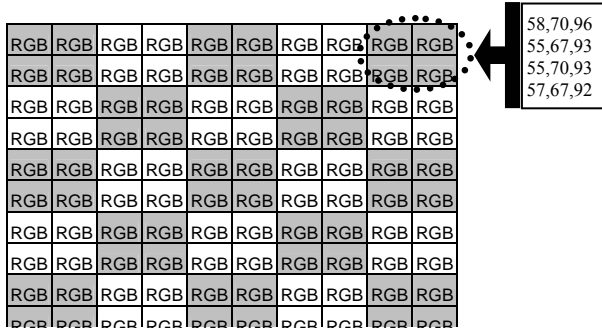


Figure 2: 10x10 pixel frame example.

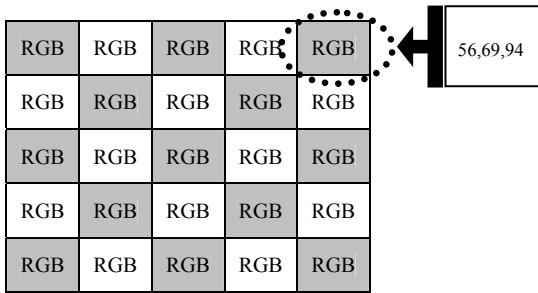


Figure 3: 5x5 pixel RGB-weighted pixel array.

The RGB-weighted mean values are then checked whether they are in the specified boundaries. A maximum and a minimum values are determined for each color weight in the selected segment. The deviation between the values can affect the capacity as well as security. In the case of high data security, the deviation should be kept as low as possible, whereas the deviation can be specified as large as possible to obtain larger capacities. Therefore, the acceptable limits are highly application specific.

Acceptable RGB values for the marked area:

Rmax : 58, Gmax: 70, Bmax : 96

Rmin : 55, Gmin : 67, Bmin : 92

Rdev : 3, Gdev: 3, Bdev: 4

$50 \leq R \leq 63$; $62 \leq G \leq 75$; $87 \leq B \leq 101$

The values found above confirms that this segment is labeled as logic 1 and the rest of segments are labeled in the same way and therefore, the segments, which can embed data, are determined. Having found appropriate segments, the ASCII codes of the data are embedded into pixels using R-weighted encoding algorithm.

2.4.2 λ Based Reduced Segmentation

The wavelength gap is determined by the help of pixels wavelength deviations (λ max and λ min) for each segment. If the wavelength gap of the segments

corresponds to a single color as shown in Table-1, that segment can be marked as “data embedding segment” and the original λ values are exchanged with weighted mean value. The procedure is repeated for all segments. The graphical explanation of the methods is given in Figure 4 and Figure 5 respectively. In Figure 4, every segment is consisted of four pixels and the λ max and λ min values of the pixels are determined.

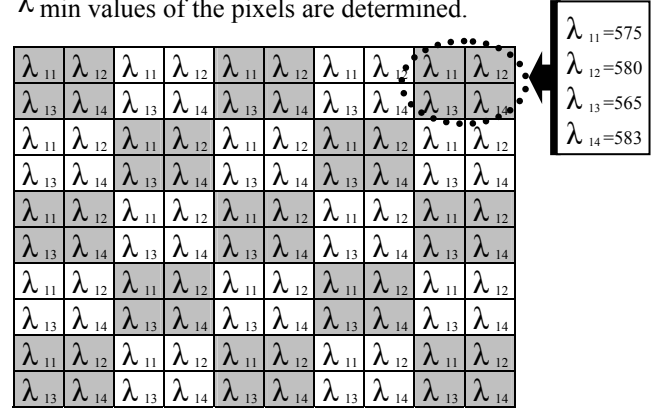


Figure 4: 10x10 raw pixel frame

λ max = 583 (Yellow wavelength)

λ min = 565 (Yellow wavelength)

$$\lambda_{\text{mean}} = \sum_{i=0}^1 \sum_{j=0}^4 \left(\frac{\lambda_{ij}}{4} \right) \quad (4)$$

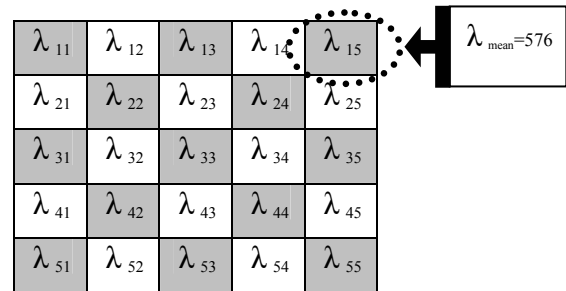


Figure 5: 5x5 wavelength based reduced pixel array.

Since λ max and λ min values obtained from Figure 4 by using Equation-4 are in the range of a single color, which is yellow in this example, the selected area can be used for data embedding.

2.4.3 R-Weighted Coding Technique

The most desired criteria for stenographic methods are: minimum corruption and maximum data embedding capacity. R-weighted encoding technique was developed in order to maintain these criteria [10].

A pixel combining with three prime colors of RGB(89,143,240) will suggest that the distribution of the

prime colors will have following color weights: R=89, G=143, B=240. As an example, an ASCII code (153) will be embedded into a pixel as shown in the Figure-6. The embedded data extraction process is illustrated in the Figure-7.

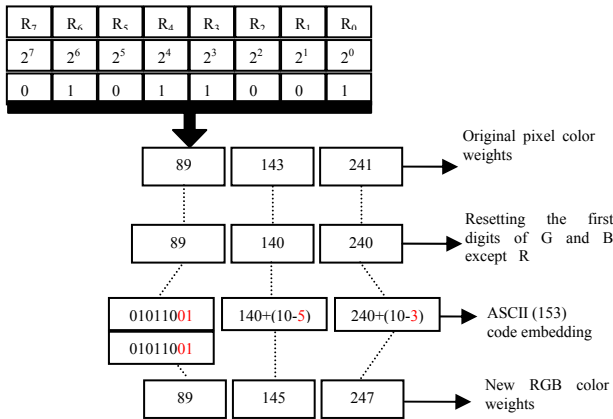


Figure 6: The process for ASCII code embedding into a pixel.

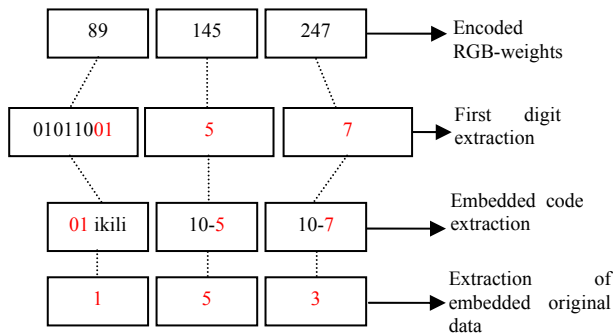


Figure 7: The data extraction process from encoded pixel.

As shown in the Figure-6, the first digits of the G and B colors are reset. Since the ASCII code ranges from 0 to 255 in decimal, the R color can hold maximum value of 2 as decimal and it can be represented 10 as binary. This incidence can be utilized as an advantage, because we will only need just 2 bits of the R color in all cases and the third digit of the ASCII code is embedded into R color's first two binary digits.

In the extraction process, first two binary digit of the R color compound of the encoded RGB is converted into a decimal digit which will generates the most significant digit of the ASCII code. The least significant digit of the G and B color weights are used to generate the whole ASCII code. The details of the extraction process are shown in the Figure-7.

It is not required to convert the embedded data into the ASCII or expanded ASCII, 8-bit EBCDIC code can be preferred instead. Encoding or embedding process is implemented according to the reference chosen and the extraction process is implemented in the same manner. In

this method the UNICODE can also be used, however, the total embedding data capacity will be half in size [9].

3 Discussion

The proposed methods include a new approach to embedding data into video streams. The contents of the frames of the video stream or an image can affect the security level. In some cases, certain files cannot assure identical security, for example, excessive color transition and regular geometric shapes can cause undesired image or video frame distortions which can be noticed by human eyes. These factors can reduce the potential segments number and consequently the data embedding capacity.

In the MPEG standard, there is no obligation for the number of frames per second. This flexibility can surely affect the data hiding capacity in negative manner or vice versa. The proposed methods not only is for watermarking purposes [6, 26], but also embedding secure data into the video stream for the purpose of communication envisages. The security level and data store capacity of the data embedding procedure is configured by a software application running the designed algorithm explained before.

4 Results

We have investigated data hiding methods to be used in video stream files i.e. MPEG and have also designed an algorithm to implement the methods proposed. Our research activities have mainly focused on RGB-weighted based encoding techniques. The proposed methods can embed as much data as 2,66 times compared to the rate of the classical LSB (Least Significant Bit) technique. Besides, in this method a unique encoding technique implemented on 'R' color values. Thus, 'R' color encoding only use 1, 2, and 3 numbers instead of whole decimal numbers as in the 'G' and 'B' color encoding. 'R' color encoding enables less deviation in the obtained pixel color, so the final encoded frame can be appeared undistorted. During the entire encoding and decoding processes all exterior noise and transmission faults are omitted.

5 References

- [1] Huiping Guo, Yingjiu Li, Anyi Liu, Sushil Jajodi, "A fragile watermarking scheme for detecting malicious modifications of database relations" Elsevier Inc. doi:10.1016/j.ins.2005.06.003
- [2] Mauro Barni, Franco Bartolini, Teddy Furon, "A general framework for robust watermarking security" Elsevier B.V. doi:10.1016/S0165-1684(03)00168-3
- [3] A. Adhipathi Reddy, B.N. Chatterji, "A new wavelet based logo-watermarking scheme" Elsevier B.V. doi:10.1016/j.patrec.2004.09.047

- [4] Rui-min Shen, Yong-gang Fu, Hong-tao Lu, “**A novel image watermarking scheme based on support vector regression**”
Elsevier Inc. doi:10.1016/j.jss.2005.02.013
- [5] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun, “**Attack modelling: towards a second generation watermarking benchmark**”
Elsevier Science B.V. PII: S0165-1684(01)00039-1/2001
- [6] E. Beşdok, “**Hiding information in multispectral spatial images**”
2005 Elsevier GmbH. doi: 10.1016/j.aeue.2004.11.040
- [7] Chung-Ming Wang, Peng-Cheng Wang, “**Steganography on point-sampled geometry**”
Elsevier Ltd. doi:10.1016/j.cag.2006.01.030
- [8] Young-Won Kim, Il-Seok Oh, “**Watermarking text document images using edge direction histograms**”
Elsevier B.V. doi:10.1016/j.patrec.2004.04.002.
- [9] “**Information Security Application Base on Data Hiding and Coding-PhD Thesis**”, AKAR Feyzi, Marmara University Institute of Science, 2005.
- [10] F.Akar, H.Selçuk Varol, “**A New RGB Weighted Encoding Technique for Efficient Information Hiding in Images**”, Journal of Naval Science and Engineering, Volume 2, 21–36, July 2004.
- [11] M.D. Swanson, M. Kobayashi, A.H. Tewfik, “**Embedding and Watermarking Technologies**”, Proc.of the IEEE, vol. 86, no. 6, 1064–1087, 1998.
- [12] Lee, K.-F., “**Automatic Speech Recognition: The Development of the SPHINX SYSTEM**”, Kluwer Academic Publishers, Boston, 1989.
- [13] E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand, “**Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense**”, at best, Proc. Information Hiding Workshop, pp. 7–21, 1996.
- [14] D. Gruhl, W. Bender, and A. Lu., “**Echo Hiding, Proc. Information Hiding Workshop**”, pp. 295–315, 1996.
- [15] Bin Zhu, Mitchell D. Swanson, and Ahmed H. Tewfik, “**Image Coding By Folding**”
0-8186-8183-7/97 1997 IEEE
- [16] Bin Zhu, Marshall Ramsey, and Hsinchun Chen, “**Creating a Large-Scale Content-Based Airphoto Image Digital Library**”
IEEE Transactions On Image Processing, Vol. 9, No. 1, January 2000
- [17] Bin Zhu, Member IEEE, En-hui Yang, Member IEEE, and Ahmed H. Tewfik, Fellow IEEE, “**Arithmetic Coding with Dual Symbol Sets and Its Performance Analysis**”
IEEE Transactions On Image Processing, Vol. 8, No. 12, December 1999
- [18] J. J. Chae, D. Mukherjee and B. S. Manjun, “**Color Image Embedding using Multidimensional Lattice Structures**”
0-8186-8821-1/98 1998 IEEE
- [19] Wen-Nung Lie, and Li-Chun Chang, “**Data Hiding In Images With Adaptive Numbers Of Least Significant Bits Based On The Human Visual System**”
0-7803-5467-2/99/ 1999 IEEE
- [20] “**An Adaptive Compressed MPEG-2 Video Watermarking Scheme**”, Satyen Biswas, Member, IEEE, Sunil R. Das, Life Fellow, IEEE, and Emil M. Petriu, Fellow, IEEE
- [21] Pik Wah Chan, Student Member IEEE, Michael R. Lyu, Fellow IEEE, and Roland T. Chin, “**A Novel Scheme for Hybrid Digital Video Watermarking: Approach, Evaluation and Experimentation**”
IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, No. 12, December 2005.