

Hardware Simulation of Digital Watermarking for Video

Dheeraj Shinde¹, Ramesh Y. Mali²

Student, Electronics & Telecommunication, MITCOE, Pune, India¹

Professor, Electronics & Telecommunication, MITCOE, Pune, India²

Abstract: Different digital watermarking (WM) techniques for still images have been studied in the last many years. Recently, a lot of new WM schemes have been suggested for other types of digital multimedia data, such as text, audio and video. The technology which is implemented in our work for the invisible video watermark will work according to the video frame using the Least Significant Bit (LSB) algorithm. This technique has been realized using VHDL. The system simulated on the ModelSim. The simulation results have been demonstrated. Watermark is successfully extracted at the output of extraction model.

Keywords: Digital video, WM, LSB, VHDL, ModelSim.

I. INTRODUCTION

In the past, duplicating art work was quite complicated and needed a high level of expertise for the counterfeit to look like the original. However in the digital world this is not true anymore due to a fast migration that took place from analog media to digital media during the recent decades. The digital media enabled a lot of new features for copying, editing and storage of multimedia contents. Sharing and storage of digital video data has become much easier and faster due to rapid growth of digital signal and multimedia processing. Unfortunately, this progress is also associated with various security threats and attacks i.e. image or video copying, tampering, ownership theft, unauthorized playback etc. [1].

These attacks can be performed in the twinkling of an eye using various digital devices. This particular issue become more significant when the video sequence is used as proof. In this type of cases, we need to prove that the video data is original and reliable. Thus the authentication of digital media information (Video, Audio, Image) is an important matter of concern. Digital watermark is a process to insert hidden information in digital multimedia data by signal processing method like LSB. The idea behind digital watermarking is to make use of human's insensitive perceptual organs and redundancy in digital signal. This embedded information can survive after fighting back some attacks to meet the copy right authentication and copyright protection functions that are one of the watermark applications as shown in Fig. 1.

Digital watermark doesn't change digital products' basic characteristic [2], [3]. Now a day's digital video watermarking techniques are widely used in various image or video applications such as copyright protection, data integrity, copy control, content authentication etc.[2].

Number of watermarking algorithm are available some them are operating in frequency domain, where the pixel value are transformed in to another domain by applying DWT, DCT, DHT & OCT. We may use spatial domain to provide algorithm that operate directly on the pixel values of the host image such as the Least

Significant Bit (LSB) substitution. For valid watermarking technique, it needs to satisfy three important properties namely:

- **Perceptual invisibility.**
- **Robustness against various image processing attacks.**
- **Security** [4].

In this paper, a video watermarking technique is proposed to insert invisible watermark on video in spatial domain using LSB algorithm. Hardware realization using VHDL & simulation on ModelSim was done. The paper is organized as follows: section II, LSB algorithm, section III, illustrates proposed method, section IV, Scheme of Implementation, section V, Results, and finally in section VI Conclusion is drawn.

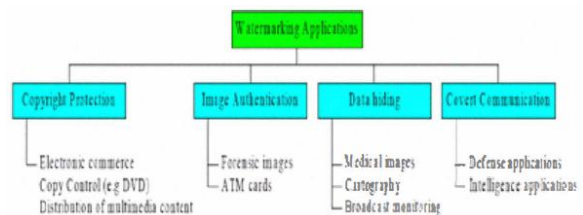


Fig. 1 Classification of watermarking technology based on applications.

II. LEAST SIGNIFICANT BIT

There are many algorithms available for invisible digital watermarking. The simplest algorithm is Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is over written with a bit from the watermark. In a digital image, information is inserted directly into every bit of image information in less perceptible parts of an image. This method is based on the pixel value's Least Significant Bit (LSB) modifications [8]. Fig. 2 illustrates simple LSB techniques for image. For the video same principle is applicable but instead of image there is a frame.

For the embedding it is effective and simple if we use a greyscale bitmap image. We required read it and then

add the data in the least significant bits of each pixel, by pixel to pixel. The greyscale image consists of 64 pixels and each pixel is represented by one byte consisting of 8 bits. It means 256 gray colour values between black and white. For black it is 0 and 255 for white. The simple principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If encoding of data would be only the last two significant bits (which are the first and second LSB) of each colour component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures [5]. For this example only the least significant bit of each pixel is used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underlined pixel.

Features of LSB (Least-Significant-Bit) [8]

- It is simple to understand
- Easy to implement

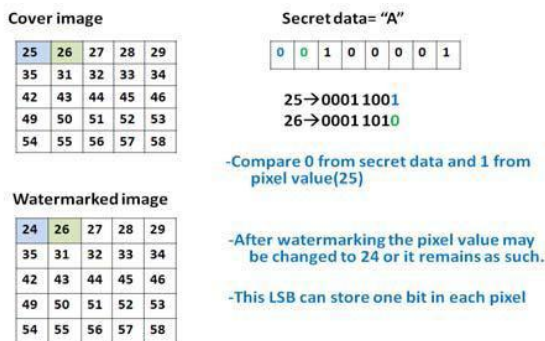


Fig. 2 Representing LSB Technique [8]

In this algorithm we embed the most significant bits of each pixel of the watermark in the least significant bit places of the original image. The embedding of the watermark is performed by choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. [7]

In the extraction we extract the most significant bits of the watermark that we embedded in the original image. Or in other words extraction of the watermark is performed by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the watermark is detected. The extracted bits do not have to exactly match with the inserted bits. A correlation measure of both bit vectors can be calculated. If the correlation of extracted bits and inserted bits is above a certain threshold, then the extraction algorithm can decide that the watermark is detected. [7] The algorithm flow chart is shown in Fig.4

III. PROPOSED METHOD

Fig. 3 shows the 1-bit LSB. In Fig. 3, the pixel value of the cover image is 141(10001101)₂ and the secret data is 0. It applies to LSB-1 that the changed pixel value of the cover is 140(10001100)₂. LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes

of embedded data. Proposed method based on LSB technique, we propose a new watermarking algorithm.

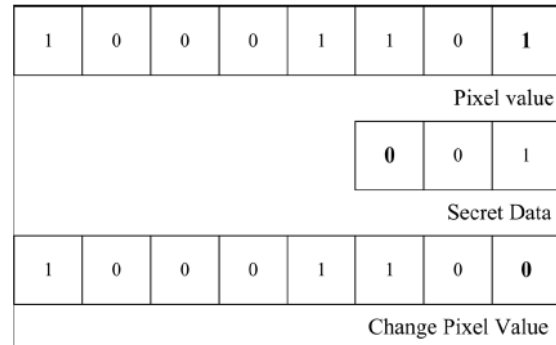


Fig. 3 Example of LSB

Most of researchers have proposed the first LSB and the third and fourth LSB for hiding the data but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data, and using the RGB watermark image embedding in blue component of original image because of less sensitivity. This is because of the security reason. So, no one will expect that the hidden data in the third and the fourth LSB. [7]

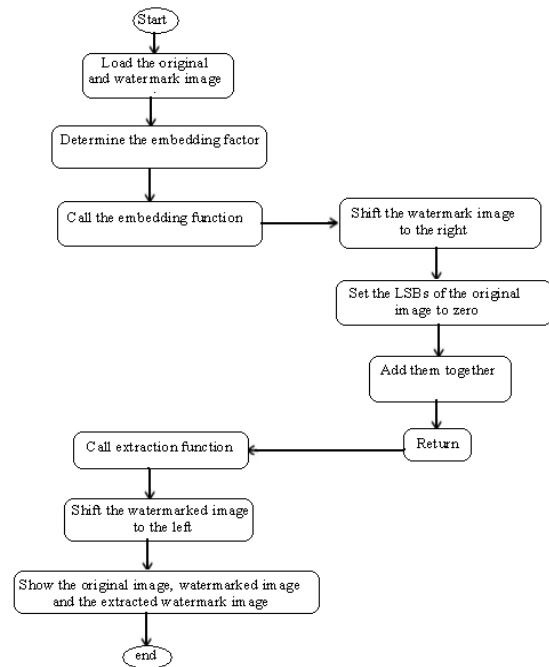


Fig.4 Flow chart of LSB algorithm [6]

Fig. 5 shows the framework of the proposed method. First, we select the image which is a colour image and we will transfer the data to binary value after typing it. Then, we hide the data in the image using the proposed algorithm. [7]

IV. SCHEME OF IMPLEMENTATION

The system consists of following units:

- Original Video block
- Watermark Image block
- Watermark Embedding block

- Watermark Extraction block
- Extracted Watermark Image block

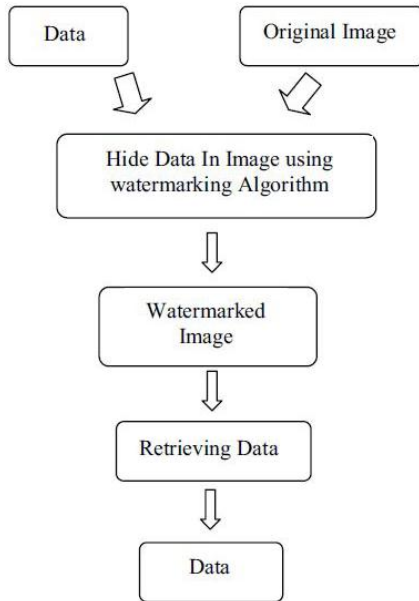


Fig. 5 The framework of the proposed method [7]

Fig.6 shows the block diagram of the project. A brief explanation of each block can be given as, Original video is the video which is to be watermarked or secured. Watermark image is image to be embedded on the original video. The watermark Embedding will insert the watermark according to algorithm and make the video content secure. The embedded information can be extracted as and when required to prove the authenticity of the owner by the use inverse procedure as that of embedding procedure. Finally extracted watermark can be stored and shown whenever required

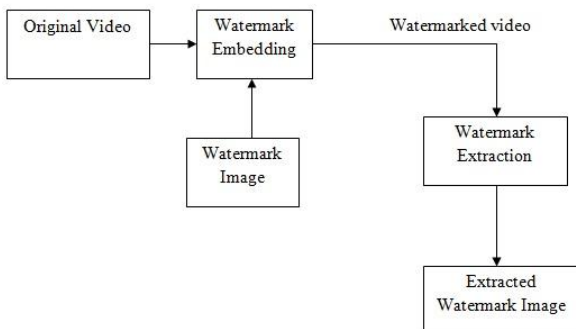


Fig .6 Block diagram of proposed system

V. RESULTS

We have seen the embedding method, block diagram. Now let's concentrate on the results. We get results at the output of different block. The watermark embedding block will be responsible for adding the hidden information on the host data (video in our case). This will generate the output video which is secured and can be transmitted over the internet. Whenever the question of authenticity arises, one can decrypt the watermark with the help of watermark extraction by doing the inverse procedure as that of embedding. Finally, the original watermark can be

received at the output of extraction block. The following figures show the watermarked frame. The LSB encryption is performed in VHDL. The results images are shown as follows in Modelsim as well as video frame, watermark.



Fig. 7 Original video frame

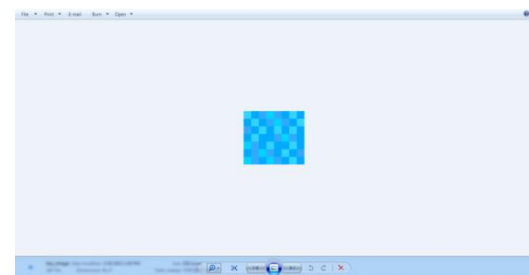


Fig. 8 Original Watermark

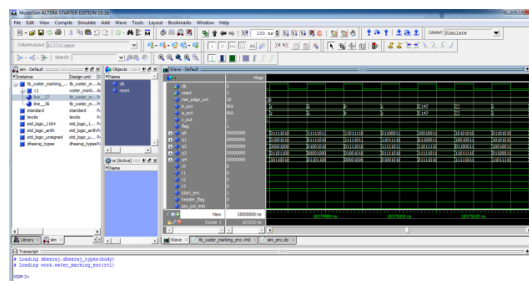


Fig. 9 ModelSim output after watermarking



Fig. 10 Watermarked video frame

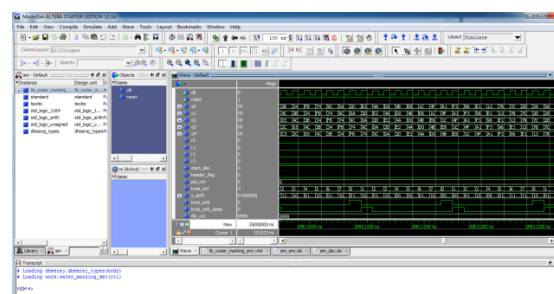


Fig. 11 ModelSim output after Decryption of watermark



Fig.12 Extracted watermark

VI. CONCLUSION

We have successfully implemented the LSB watermarking algorithm and embedded the watermark in the video. The encrypted video is given to the watermark extraction where the extraction procedure is done. Finally the original watermark information is extracted at the output which matches with the original watermark. Thus the LSB algorithm provides confidentiality, data integrity and authentication. Hence the transmission over internet is said to be secure. Authenticity of owner can be verified whenever required. The security of digital multimedia data has been a major research topic in the recent years and many academic and industry persons are trying to work in these areas to bring optimistic results.

REFERENCES

- [1] X. Li, Y. Shoshan, A. Fish, G. A. Jullien, and O. Yadid-Pecht, "Hardware implementations of video watermarking," *International Book Series on Information Science and Computing*, no. 5, pp.9-16, June 2008.
- [2] G. Zhu, N. Sang, "Watermarking Algorithm Research and Implementation Based on DCT Block," *World Academy of Science, Engineering and Technology*, 45, 2008.
- [3] V. Potdar, S. Han and E. Chang, "A survey of Digital Image Watermarking Techniques," *3rd International IEEE Conference on Industrial Informatics, Perth, Western Australia*, pp. 10-12, Aug 2005.
- [4] Wessam S. ElAraby, Ahmed H. Madian, Mahmoud A. Ashour and Abdel M. Wahdan, "Hardware Realization of DC Embedding Video Watermarking Technique based on FPGA", *22nd International Conference on Microelectronics (ICM 2010)*
- [5] H. Arafat Ali, "Qualitative Spatial Image Data Hiding for Secure Data Transmission", *GVIP Journal*, Volume 7, Issue 2, pages 35
- [6] Mona M. El-Ghoneimy, "Comparison Between Two Watermarking Algorithms Using Dct Coefficient, And Lsb Replacement", *Journal of Theoretical and Applied Information Technology*
- [7] Rajni Verma and Archana Tiwari, "Copyright Protection for Watermark Image Using LSB Algorithm in Colored Image", *Advance in Electronic and Electric Engineering*, ISSN 2231-1297, Volume 4, Number 5 (2014), pp. 499-506
- [8] Rajni Goyal and Naresh Kumar, "LSB Based Digital Watermarking Technique", *International Journal of Application or Innovation in Engineering & Management (IJAEM)*, ISSN 2319 - 4847, Volume 3, Issue 9, September 2014