A Survey of Hardware Implementation for Video Watermarking

Dheeraj Shinde[1] Ramesh Y. Mali[2]
[1,2]Department of Electronics & Telecommunication Engineering
[1,2]MIT College of Engineering, Pune, India

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. Brief overview of existing digital video WM is presented in this paper. Classifications of WM techniques are discussed. Every WM application has its own specific requirements; WM design needs to take the intended application into consideration. Various video WM applications are discussed in the paper. Various watermarking attacks are discussed at the end of paper.

Key words: Digital video, WM, FPGA, Video surveillance (VS), ASIC

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. [2]. These attacks can be performed in the twinkling of an eye using various digital devices. This particular issue becomes 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 watermarking, a data hiding technique is one of the key authentication methods [2]. 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]. For video authentication, watermarking conforms that the original content has not been changed or manipulated. The implementation of hardware WM is usually done on custom-designed circuitry, i.e. application specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs).The overall advantage of hardware implementation over the software implementation is in terms of lower power consumption, reduced area and reliability Therefore; it may be more suitable for real time applications.

Paper organization is as follow: In Section II, we will introduce video watermarking. In Section III, we survey different works related with hardware implementation of watermarking for various application. In Section IV, various applications of video watermarking are presented with example. In Section V, different types of attacks on watermarking are considered. Finally, in Section VI, we conclude the paper.

II. VIDEO WATERMARKING

Watermarking techniques can be classified into various categories. The general classification of watermarking techniques is shown in fig.1. According to level of robustness, the WM can be categorized into three main divisions:

- Fragile Watermarking
- Semi- fragile Watermarking
- Robust Watermarking

Watermark is said to be fragile if it is not detectable even after the slightest modification and a watermark is called robust if it oppose an intended class of transformations. By programming the code and application of available software tools, it became easy to design and implements any WM algorithm at various levels of complexity. Semi fragile watermarking is intermediate of both. It can be used for surveillance camera application.

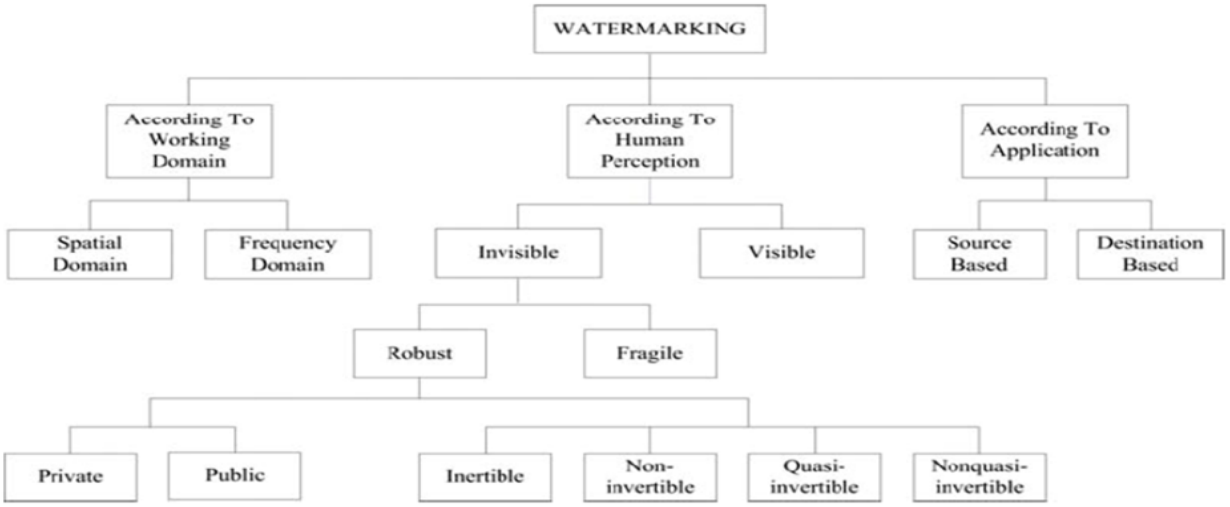

Fig. 1: Classification of existing watermarking [2]

According to the domain in which video WM is performed, WM processing methods can be classified into two categories

- Spatial domain
- Frequency domain.

In the spatial domain, minor changes to the values of the pixels in a minor way can be directly applied. Embedded information through this technique is hardly noticeable to the human eye. For example, pseudo-random WM works by a simple addition of a small amplitude pseudo-noise signal to the original media data.

In the frequency domain, the object first goes through a certain transformation, like DCT or (DWT). Then WM is embedded in the transform coefficients to add identifying information after that it is inversely transformed to receive the watermarked data. The frequency domain methods are more resilient than the spatial domain techniques.

According to application point of view, digital WM is divided in two types:

- Source based[3]
- Destination based [3]

Source based WM is generally used to authenticate whether a received media data has been manipulated and the destination based WM is used track the source of illegal copies.

III. Literature Survey

Contrary to still image watermarking techniques, new problems and new challenges have emerged in video watermarking applications.

Shoshan et al. [4] and Li et al. [2] described an abstract of the different existing video watermarking techniques and showed their features and specific requirements, possible applications, benefits and drawbacks. From the past few years, researcher has been focusing on efficient watermarking systems implementation using hardware platforms. They vary in terms of applications and implementation platforms.

Strycker et al. [5] proposed a well-known video watermarking scheme, called Just Another Watermarking System (JAWS), for television (TV) broadcast monitoring and implemented the system on a Philips's Trimedia TM-1000 Very Long Instruction Word (VLIW) processor. Experimental result showed the feasibility of watermarking in a professional TV broadcast monitoring system.

Mathai et al. [6]-[7] presented an Application Specific Integrated Circuits (ASIC) implementation of the JAWS watermarking algorithm using 1.8V, 0.18µm complementary metal oxide semiconductor (CMOS) technology for real-time embedding in video stream. They showed, with a core area of 3.53 mm^2 and operating frequency of 75MHz, watermarking of raw digital video stream at a peak pixel rate of over 3 Mpixels/s while consuming only 60 mW power.

Mohanty et al. [8] introduced a concept of secure digital camera (SDC) with a built-in invisible-robust watermarking and encryption facility.

Jeong et al. [14] presented HAAR-wavelet-based real time video watermarking with the help of a FPGA prototype.

A real-time watermarking system for video using DSP and VLIW processors was presented by Petitjean et al. [15], which embeds the watermark using fractal approximation.

Very few work on hardware based video watermarking for the surveillance application had done.

In [9] Schyndel et al. presented a watermarking system based on spread spectrum watermarking generated by the array construction method. They focused on surveillance video watermarking.

Shoshan et al.[16] designed and implemented hardware architecture of a watermarking system for still image authentication based on JPEG encoding process.

Roy et al. [1] presented the design and implementation of hardware based invisible and semi-fragile video watermarking system for video authentication with the help of non-standard MJPEG coding method.

IV. Applications of Video WM

This section presents various applications in which digital WM can bring a valuable support in the context of video data. The following main watermarking applications are considered in the open literature and as commercial applications.

Applications	Purpose
Copyright protection	To prove the ownership
Video authentication	To make sure that the original content has not been altered
Copy control	To Prevent unauthorized copying
Broadcast monitoring	To identify the video item being broadcasted

Table 1: Video WM: Applications and Purposes

A. Video Authentication:

Popular video editing software easily allows tampering with video content and hence it is not reliable anymore. Authentication techniques are consequently needed in order to ensure the authenticity of the content. One solution is the use of digital WM.

Fig. 2 shows, a sketch of a simple video surveillance (VS) system, in which WM is used to authenticate VS data, is given [13]. Timestamp, camera ID and frame serial number are used as a watermark, embedded into every single frame of the video stream. The central unit is responsible for analysis of the watermarked sequences and giving an indication whenever a cynical situation is noticed, and then may either be sent to the security service or compressed for storage. When needed, the stored video sequence may be used as valid evidence in court. It is possible to reflect any manipulation by detecting the watermarks. The motive to keep the computational complexity less depends on the implementation method as well as application. In real time applications, computations are required to be done in a very less time. The speed and processing power of the selected hardware platform, restrict the algorithm level of complexity which is to be computed in a given time frame. When implementing in hardware, higher complexity requires additional hardware which means more area and additional costs.

However, each additional feature, added to the algorithm, enhance the computational effort and hardware

resources used for calculations. Hence, an effective method will consist of the minimum number of features required to satisfy the needs of the application for which it is designed.

V. ATTACKS ON WATERMARKING

A. *Undetected Modifications:*

In this type of attack the attacker will try to modify the watermarked image such that it will not be detected by the algorithm. Attacker might be satisfied with making changes that will be unable to detect with a "sensible" probability or modifications that will be misunderstand by the detector, like pasting and masquerading cutting as interfering at the border of the cropped area.

B. *Information Leakage:*

Another severe problem that various authentication watermarks have is information leakage. In this problem the attacker might be interested in acquiring some information about the secret pass key, detecting synchronization patterns, entities derived from it, like a random walk through the image.

C. *Stego-Image Attack:*

In this type, the attacker has only one verified image and is interested in doing change that will be undetectable or extracting some confidential information from the scheme.

D. *Multiple Stego-Image Attack:*

In this type of attacks, the attacker has various authenticated images and is interested in making undetectable changes or retrieving information from the scheme.

E. *Verification Device Attack:*

The attacker has permission to access the verification device. The powers of this type of attack rely on the output available to the attacker. The output might be a bitmap with pixels/blocks or it might be binary Yes/No for the whole image representing it as genuine or distorted. Again, the attacker is interested in doing undetectable changes or extracting confidential information from the method.

F. *Cover-Image Attack:*

In this type of attack, the attacker has many pairs of genuine images. This assumption is reasonable if an attacker can somehow managed to access the raw images before authentication has occurred or when possible conclusion can be made about the genuine. Image semantic might be used to obtain an approximate raw image. Again, the attacker is interested in doing undetectable changes or retrieving information from the scheme.

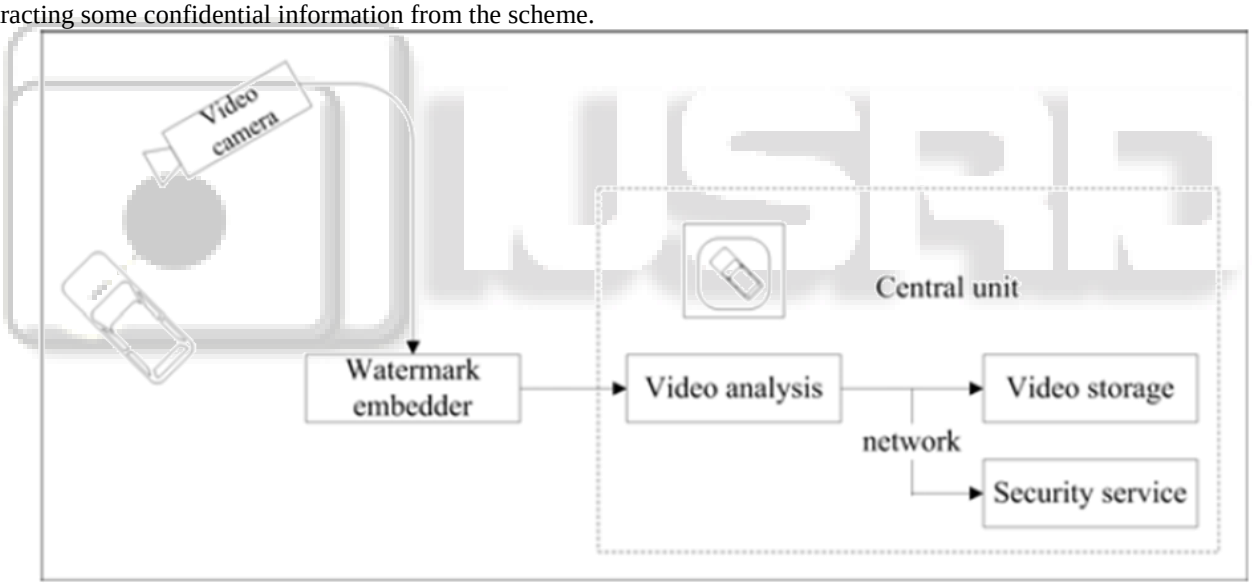

Fig. 2: WM -based authentication for automatic VS[2]

In Voloshynovskiy et al. [10], several state-of-the-art attacks are discussed. The wide class of existing attacks is categorized into four classes of attacks: removal, geometric, cryptographic and protocol attacks. A new direction of attacks based on watermarking estimation exploiting the statistics of watermarking data and original data with or without the knowledge of watermarking technology is also discussed in the same paper. The analysis concentrates on copyright protection of still images.

Jayamalar et al. [11] also categorized digital watermarking attacks as follows: subtractive, distortive, additive, filtering, cropping, compression, rotation and scaling, statistical averaging, multiple watermarking attacks, etc. Most of these attacks coincide with the attacks discussed in [10].

Hollimen et al. in [12] describe a class of attacks on certain block-based oblivious watermarking schemes. They show that watermarking techniques that embed watermarks into a host image in a block-wise independent fashion are vulnerable. This attack is possible for both fragile and robust watermarking schemes.

With copyright protection applications, the purpose of the attacks is to remove the watermark from the data or to modify the watermark signal in the data so that it becomes undetectable and the owner's information from the original data is lost. This has to be done without degrading the original information in the data otherwise the purpose of the attack is not served.

On the other hand, with authentication in surveillance cameras, the goal of the watermarking scheme is that if any sort of alteration is done in the watermarked data, the watermark detector will be unable to detect the watermark, indicating that the original watermarked data has been tampered. Hence, the attacker's goal is to modify the

captured data by the surveillance camera without altering the watermark. Therefore, the attacks on robust watermarking are not necessarily effective on semi-fragile watermarking targeted to authentication purposes. In this case, the attacker might try to extract the watermark information from the watermarked data and use that within their false data to make it authenticated.

The attacker has two possible ways of attacking the watermarking system: offline attack and online or real-time attack. We discuss both of these below.

G. Offline Attack:

An offline attack refers to an approach in which the attacker computes validly-watermarked fraudulent video offline. This may involve collecting a series of watermarked video frames for a long period of time. The attacker might be able to extract an extended watermark sequence based on a statistical analysis of those video frames. The statistical analysis of the video frames to extract the original watermark sequence embedded into the frames might be similar to the estimation based attack on the watermarked frames, described in [10]. The collected video frames can be a long video sequence of a static scene depending on the algorithm of the statistical analysis. After extracting the extended watermark sequence the attacker must determine how to embed a new watermark sequence into his own video in such a way that it will pass the verification algorithm performed in the base station. The watermark sequence extracted from the video will not suffice, as the corresponding sequence of pseudorandom bits generated by the watermarking algorithm will not repeat, assuming the secret key and algorithm are chosen appropriately. However, the attacker may be able to use this information to mount an attack on the pseudorandom number generator, enabling him or her to predict watermark sequences and forge valid watermarked video.

H. Online Attack:

An online attack means the attacker has to perform all the computation for generating the watermark sequence in real-time. In this attack he performs a brute force attack on the current watermarked video frame. He may perform the attack in a block-wise manner to reduce the computation. The attacker requires access to un-watermarked versions of the image blocks he wishes to attack - the feasibility of this assumption is addressed below. A single watermarked video frame can be divided into different watermarked pixel blocks of a particular size (i.e. 8 × 8 pixels). To tamper with a particular region of a video frame the attacker performs the brute-force attack only for that particular watermarked block of the frame. The attacker guesses every possible permutation of the original watermark sequence of that particular block. Then using the watermarking algorithm he applies each of the guessed watermark sequences to the original un-watermarked video frame. By comparing the results to the watermarked version of the block, the attacker can determine the watermark or retrieve secret information from scheme.

VI. CONCLUSIONS

In this paper background of video WM techniques is provided. Various methods of hardware implementation of video watermarking with different watermarking algorithms are reviewed. Various applications of video WM are discussed. Simple video surveillance example is explained to understand the concept of video authentication. We have discussed various attacks which are affecting some of the famous watermarking techniques.

REFERENCES

[1] S. D. Roy, X. Li, Y. Shoshan, A. Fish and O. Yadid-Pecht, “Hardware Implementation of a Digital Watermarking System for Video Authentication”, IEEE Transactions of Circuits and Systems for Video Technology, vol. PP, no. 99, pp. 1, 2012.

[2] 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.

[3] Sin-Joo Lee, and Sung-Hwan Jung, “A survey of watermarking techniques applied to multimedia”. IEEE International Symposium on Industrial Electronics, Korea, June 2001. Vol. 1, pp. 272 – 277.

[4] Y. Shoshan, A. Fish, X. Li, G. A. Jullien, and O. Yadid-Pecht, “VLSI watermark implementations and applications,” International Journal on Information Technologies and Knowledge, vol. 2, no. 4, pp. 379–386, June 2008.

[5] L. De Strycker, P. Termont, J. Vandewege, J. Haitsma, A. Kalker, M. Maes and G. Depovere, "Implementation of a real-time digital watermarking process for broadcast monitoring on a TriMedia VLIW processor," in Vision, Image and Signal Processing, IEEE Proceedings, 2000, pp. 371-376.

[6] N. J. Mathai,D. Kundur and A. Sheikholeslami, "Hardware implementation perspectives of digital video watermarking algorithms," Signal Processing, IEEE Transactions on, vol. 51, pp. 925-938, 2003.

[7] N. J. Mathai, A. Sheikholesami, and D. Kundur, “VLSI implementation of a real-time video watermark embedder and detector,” in Proc. of IEEE Intl.Symposium on Circuits and Systems, vol. 2, 2003, pp. 772–775.

[8] S. P. Mohanty, “A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management”, in Journal of Systems Architecture, vol.55, no. 10-12, pp. 468-480, 2009.

[9] R. V. Schyndel, "A Hardware-Based Surveillance Video Camera Watermark.”, in IEEE International Conference on Digital Image Computing: Techniques and Applications (DICTA), 2010, pp. 343-348.

[10] S. Voloshynovskiy, S. Pereira,T. Pun, J.J. Eggers and J.K. Su, “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks”, in IEEE Communications Magazine, vol. 39, no. 8, pp. 118-126, 2001.

[11] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," in IEEE Transactions on Image Processing, vol. 9, pp. 432-441,2000.

[12] M. Kuttera, S. Voloshynovskiya and A. Herrigela, "The watermark copy attack," in Proc. SPIE Electronic Imaging ' 00, Security and Watermarking

of Multimedia Content II, vol. 3971, pp.371-380,2000.

[13] M. Barni, F. Bartolini, J. Fridrich, M. Goljan, and A. Piva, "Digital watermarking for the authentication of AVS data," in EUSIPCO00, 10th Eur. Signal Processing Conf., Tampere, Finland, Sept. 2000.

[14] R. McEvoy, J. Curran, P. Cotter, and C. Murphy, "Fortuna: Cryptographically Secure Pseudo-Random Number Generation in Software and Hardware", in Irish Signals and Systems Conference, 2006, pp.457-462.

[15] F. Arnault, T. Berger and A. Necer, "A new class of stream ciphers combining LFSR and FCSR architectures," Progress in Cryptology—INDOCRYPT, 2002, pp. 22-33, 2002.

[16] Fish, Y. Shoshan and O. Yadid-Pecht, "Digital Watermarking CMOS Sensors." US Patent 7 688 994, Mar. 30, 2010.

