

A Robust Digital Video Watermarking

J. Suganya Shesathri, S.K.Yaamini

Abstract-Watermarking describes that hide information in digital media such as images, audio and video. This work mainly focuses on invisible and robust watermark schemes for video sequences. A major requirement for the video watermarking schemes is the possibility of invisible watermarking and decoding with no access to the original signal. Piracy and copyright production is a major area of the in Digital Asset Management System. Encryption, Steganography, cryptography watermarking techniques was already adopted to maintain piracy and security in Digital Media such as images, audio and video. Most of the watermarking techniques focus on embedding hidden message into the Digital Media to protect the ownership of the video contents. Here, we propose an algorithm to claim the ownership of Digital Video using Dynamic watermarking techniques. This involves selection of key frames from the given Digital Video based on rgb values. Pair of key frames is analyzed for horizontal jagged noise around the edges using interlaced scanning. Finally, Spread Transform-Scalar Costa Scheme is applied over the order pair of key frames to generate watermark signal.

Keywords— watermarking, Steganography, Cryptography, Spread Transform, Scalar Costa Scheme

I. INTRODUCTION:

Watermarking is about robustness against possible attacks, Watermark need not be hidden. Video Watermarking involves embedding hidden information derived from frames of video contents. Digital media are now common after having taken over the traditional analog media. There are lots of numbers of technical reasons favoring to the digital media. Infrastructure such as computers, printers, digital media players, and huge rate digital transmission facilities became inexpensive and widely available. Digital networks also provide an efficient cost-effective means of distributing digital media. The quality of the digital media is very good; in most cases it is far better than corresponding analog coding. Different types of compression techniques and error correction codes that are now available for data digital representation improved the quality-storage space tradeoffs. However a major problem of digital media distribution schemes is the difficulty to protect ownership rights or to trace the source of a digital file. Digital media are easily copied and redistributed by unauthorized parties. Anyone may propose to use hidden codes to defend the media, but when the media is decoded for viewing it is synchronized into data streams that can be copied. Data hidden directly in the host signal can serve as concern means for authentication. Imperceptible hiding of data in the digital media is called watermarking and the embedded information is called a watermark.

Manuscript published on 30 April 2013.

* Correspondence Author (s)

J. Suganya Shesathri, PG Scholar, Department of Information Technology, K.L.N College of Information Technology, Sivagangai, India.

S.K.Yaamini, PG Scholar, Department of Information Technology, K.L.N College of Information Technology, Sivagangai, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Many groups developing video watermarking technology have applied image watermarking technology into frames of a digital video content. Unfortunately, this means that each frame has a distinct watermark unrelated to the preceding and following frames, which may be visually very similar. A frequent attacker can take advantage of this by averaging frames to discover, and remove, this watermarking technology does not calculate watermarks based on individual frames, but on selected prisms, so it does not provide attackers with this opportunity. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible.

II. RELATED WORKS

Many of the watermarking schemes have been proposed in the literature for still images and videos. Most of them operate on uncompressed videos, while others embed watermarks directly into compressed video. the watermark must be either robust or fragile, depending on the application. By "robust" we mean the capability of the watermark to resist manipulations of the media, such as lossy compression where compressing data and then decompressing it retrieves data that may well be different from the original, but are close enough to be useful in some way. Further, the novel quantization-based on data-hiding method, named Rational Dither Modulation (RDM) is presented. [1] This method gives most of the simplicity of the dither modulation (DM) scheme, which is highly vulnerable to amplitude scaling, but changes the latter in some way that it becomes invariant to get attacks. RDM is using a gain-invariant adaptive quantization step-size at embedded and also decoder. This causes the watermarked signal being asymptotically stationary. The problem in this paper is RDM can only work in the scalar fashion. An encryption method and with the novel property that publicly revealing an encryption key does not reveal the corresponding decryption key.

Digital watermarking permits linking information on documents that means that key information is written twice on the documents. Couriers or other secure means are not needed to transmit keys, as a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only recipient can decipher the message, because he only knows the desired decryption key. A message can be signed using a privately held decryption key. Anyone can verify this signature using the corresponding publicly known the encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in electronic mail and electronic funds transfer systems.

The problem in this paper [2] is implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers and the reader is urged to find a way to break the system.

Robust and secure digital signature solution for multimedia content authentication, by integrating content feature extraction, error correction coding (ECC), watermarking and cryptographic signature into one unified framework the problem in this paper is [3] low robustness in image processing. . Information theoretic bounds and simulation results with state-of-the-art coding techniques are compared. Further, reception after amplitude scaling attacks and the inevitability of SCS embedding are investigated. [4] The later result is mainly due to the independence of SCS from the characteristics of the original signal.

RDM is based on using a gain-invariant adaptive quantization step-size at both embedded and decoder. This causes the watermarked signal being asymptotically stationary but [5] those algorithms based on spherical code words, which are quite difficult to deal with the attacks. Spread Transform (ST) is a quantization watermarking algorithm in which vectors of the wavelet coefficients of a host work are quantized, using one of two dithered quantizes, to embed hidden information bits. Visibility considerations require that each spreading vector refer to corresponding pixels in each of several frames [6] this paper enables, it is tough to develop adaptive coding and modulation techniques.

Robust watermarking Techniques for color images are a Digital Signal or pattern inserted into a digital image. Here embedded the watermark in the phase information in the discrete Fourier transform domain since the phase distortion is more sensitive to HVS than magnitude distortion. Therefore it is more robust to tampering when compared to magnitude distortion. This paper enables that the contains linear additive watermarks, few algorithms resist the watermark copy attack and ambiguity attack. The problem of in this paper [15] is low robustness to product the copyright and privacy.

III.SYSTEM ARCHITECTURE

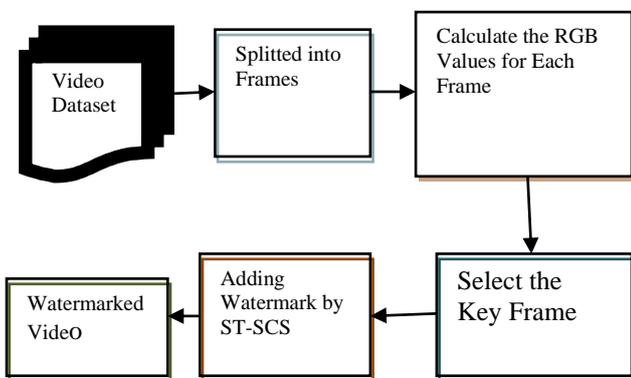


Fig1. Watermark generated and embedded into the video content

IV.PROPOSED SYSTEM

This concept gives the clear view over sequence of multiple image leads to video rendering. If an image in the video is preprocessed well so as the video. Here the video quality is based on video preprocessing. While image watermarking already entered in real time, video watermarking has not

became popular yet. This because of the fact that the problem is difficulty and usually requires strengthful computation resources. It is most important to note that video watermarking is even more useful than image watermarking. Illegal distribution of movies through internet is one of the biggest problems of the content owners. Another problem is broadcast hijacking, which is usually done on the TV broadcasting of video.

A. Watermark Embedding

In our proposal, first we segmented the video into frames, then selecting and ordering of the frames by using Rgb values. After that similarity ratio was found and ST-SCS technique is used to generate the watermark. The generated watermark is embedded into our video content; finally we obtained the watermarked video content.

$$W = U_0 - \alpha X = \alpha q \quad (1)$$

$$S = X + W \quad (2)$$

Scalar Costa Scheme (SCS), which is a suboptimal technique using scalar embedding and reception, functions. Information theoretic bounds and simulation results with state-of-the-art coding techniques are compared.

$$q = Q_{\Delta} \left\{ x_n - \Delta \left(\frac{d_n}{D} + k_n \right) \right\} - \left(x_n - \Delta \left(\frac{d_n}{D} + k_n \right) \right) \quad (3)$$

Where Q_{Δ} denotes the scalar uniform quantization.

Applying ST-SCS watermarking technique directly to the video frames. Here frames are divided into number of pixels and then the embedder computes the DCT into video frames after that the actual watermark

Values added to the video frames. Thus, the achievable rate of ST-SCS might be larger than that of SCS. Note that ST-SCS can never perform worse than SCS since SCS is a special case of ST-SCS with the optimum choice of the spreading factor for attacks of differing noise powers is investigated.

V.EXPERIMENTAL RESULTS

In our experiment, we have tested the original video content shown in Table1 .The frame size of the original video content is 256×240 where the size of the watermark is 52×19 pixels. The result shows that there are no quality degradation. Set of possible attacks is very complicated and can't be easily described. Neither can we define a limit on the distortion introduced by signal processing operations in general case. Nowadays there have been published more number of articles that contain information theoretic analysis of information hiding techniques. Such analysis is important as it provides us theoretic boundaries of performance and intuition. The quality of the watermarked video content obtained by using peak noise ratio signal values .it could be obtained with respect to the original video content.



TABLE 1: Embedding the watermark into the original video content

WATERMARK EMBEDDING ALGORITHM	ORIGINAL VIDEO	WATERMARK	WATERMARKED VIDEO	PSNR VALUE
SPREAD TRANSFORM-SCALAR COSTA SCHEME		Copyright		0.7432
SPREAD SPECTRUM		Copyright		0.9854
QIM		Copyright		0.8535
DFT		Copyright		0.8586

$$PSNR = 10 \log \left[\frac{\max(I(i, j)^2)}{\sum_{N, M} (I(i, j) - I(i, j))^2} \right] \quad (4)$$

VI. CONCLUSION AND FUTURE WORK

In this paper, we focused on invisible and robust watermark schemes for video sequences. An important requirement for the video watermarking techniques is the possibility of blind watermarking. Watermarking with no access to the original signal. Privacy and copyright is a major area of concern in Digital Asset Management System. here we proposed the ST-SCS algorithm can be given good performance in the high rate of WNR and also improve the quality of video screen shots without losing the information of the sequences of images .In this phase we have completed the module till the embedding the watermark into video frames. Our proposed method of dynamic algorithm techniques for embedding the watermark to make the system highly robust and secure. The current proposed system can further be extended to the design a high compact. Our future work is to extract the water from the video frames to ensure the original watermark and the extracted watermark as same as what we are embedded in the video frames.

REFERENCES

- [1] A. V. Subramanian, Sabu Emmanuel, *Member, IEEE*, and Mohan S. Kankanhalli, *Senior Member, IEEE* " Robust Watermarking of Compressed and Encrypted JPEG2000 Images" IEEE Transactions On Multimedia, Vol. 14, No. 3, June 2012.
- [2] Ji-Won Lee1, Min-Jeong Lee2, Hae-Yeoun Lee3 and Heung-Kyu Lee "Screenshot Identification By Analysis Of Directional Inequality Of Interlaced Video" EURASIP Journal on Image and Video Processing, 2012.
- [3] Mei Jiasheng1, Li Sukang1 and Tan Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT" Proceedings of the International Symposium on Web Information Systems and Applications, May 2009
- [4] Qibin Sun and Shih-Fu Chan, "A Robust and Secure Media Signature Scheme for JPEG Images" Special Issue for MMSP, may 2002
- [5] Majid Rabbani, Rajan Joshi " An overview of the JPEG2000 still image compression standard" Signal Processing: Image Communication, 2002
- [6] Raphael C.-W. Phan · Bok-Min Goi · Geong-Sen Poh · Jongsung Kim " Analysis of a Buyer-Seller Watermarking Protocol for Trustworthy Purchasing of Digital Contents" Wireless Pers CommunSpringer Science+Business MediaDecember 2009.

- [7] J. P. Prins, Z. Erkin, and R. L. Lagendijk "Anonymous Fingerprinting with Robust QIM Watermarking Techniques" Hindawi Publishing Corporation EURASIP Journal on Information Security, October 2007.
- [8] Byung-Ho Cha and C.-C. Jay Kuo "Anti-Collusion Fingerprinting With Scalar Costa Scheme (SCS) and Colluder Weight Recovery" Ming Hsieh Department of Electrical Engineering and Signal and Image Processing Institute
- [9] Leonardo T. Duarte, *Student Member, IEEE*, Bertrand Rivet and Christian Jutten, *Fellow, IEEE* "Blind Extraction of Smooth Signals based on a Second-Order Frequency Identification Algorithm" *IEEE Signal Processing Letters*, 2010
- [10] S.M. Ramesh, Dr. A. Shanmugam "Compressed-Domain Watermarking Algorithms: A Review" *IJCST Vol. 2, Issue 1, March 2011*
- [11] Tiziano Bianchi, Alessandro Piva, and Mauro Barni "Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals" *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, March 2010
- [12] Esam A. Hagra, M. S. El-Mahallawy, A. Zein Eldin, M. W. Fakhr "Robust Secure And Blind Watermarking based On Dwt Dct Partial Multi Map Chaotic Encryption" *The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.4, November 2011*
- [13] Joachim J. Eggers, Robert Bäuml, Roman Tzschoppe, and Bernd Girod, *Fellow, IEEE* "Scalar Costa Scheme for Information Embedding" *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, April 2003
- [14] xinyu tang, 1 bonnie kirkpatrick, 2 shawna thomas, 1 guang song, 3 and nancy m. amato, "using motion planning to study unfolding kinetics" *Journal Of Computational Biology* volume 12, number 6, 2005
- [15] Amit Phadikar, "Robust Watermarking Techniques for Color Images" April 2009