Expert Systems With Applications 63 (2016) 412–434

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system

Agilandeeswari Loganathan[a,*], Ganesan Kaliyaperumal[b]

[a] School of Information Technology and Engineering, VIT University, Vellore, 632014 Tamil Nadu, India
[b] School of Information Technology & Engineering, TIFAC-CORE in Automotive Infotronics, VIT University, Vellore, 632014 Tamil Nadu, India

ARTICLE INFO

Article history:
Received 25 May 2015
Revised 22 October 2015
Accepted 12 May 2016
Available online 13 May 2016

Keywords:
Video watermarking
Multiple watermarks
Bidirectional associative memory
Fuzzy inference system
HVS
DWT
Adaptive embedding strength
Imperceptibility
Robustness
Payload

ABSTRACT

An efficient reversible adaptive video watermarking scheme for multiple watermarks based on Bi-directional Associative Memory (BAM) Neural Networks and Fuzzy Inference System namely, Multi-BAM-FUZ scheme is proposed in this paper. The main goal of this paper is to design a robust video watermarking system which facilitates secure video transmission over a communication channel by maintaining a trade-off among imperceptibility, robustness and watermark capacity or payload. The BAM neural network supports creation of weight matrix (formed out of multiple images) and this matrix is embedded into the DWT uncorrelated mid frequency coefficients of all the components (Y, Cb, Cr) of every frames of the video with varying embedding strength 'α'. This adaptive embedding strength is generated using the Fuzzy Inference System which takes HVS characteristics such as luminance, texture and edge of each frame as an input in the DWT transform. The simulations performed on various test videos demonstrate that the proposed Multi-BAM-FUZ not only outperforms other existing methods with respect to various video degradation processes, but also maintains a satisfactory image quality, robustness and payload. It is noted that, the implementation of the novel adaptive process enhances the visual quality of about 60.97 dB in terms of PSNR and 0.9998 in terms of SSIM, robustness of about nearly 1.0000 and 0.9999 in terms of Normalized Cross Correlation (NCC) value and Bit Correction Rate (BCR) respectively against various attacks. Moreover, the proposed scheme facilitates high level of payload without affecting the imperceptibility and robustness level.

1. Introduction

The rapid development of media sharing services and internet technology has increased the distribution of digital works especially the normal videos for video conferencing, video-on-demand, entertainment videos for media communication and medical videos for telemedicine, tele surgery, tele diagnosis, etc. This in turn requires a demand for protecting such video distributions in terms of content authentication against illegitimate users. Digital watermarking (Cox, Kilian, Leighton, & Shamoon, 1997; Cox, Miller, & Bloom, 2002) is an effective technique which embeds some data (image/video) called watermark into a cover content (video) and later can be extracted to verify the originality of the content. The watermark can take its own form such as ownership identifiers (for example, Logo and fingerprint), copyright messages for normal video communication or patient's scan reports for medical video communication or any other digital formats in the form of binary, gray level or color images. This growing popularity of video based applications attracts the research towards video watermarking. The challenges over attacks in video watermarking scheme are more compared to the image watermarking. The essential characteristics of a good watermarking algorithm are the imperceptibility or transparency, authenticity, robustness and capacity or payload.

To prevent unauthorized claiming of ownership, the demand to introduce effective watermarking is very high. The probability of extracting watermark by unauthorized means or illegitimate user is reduced by means of multi-level authentication i.e. this can be possible by one or more combination of authentication techniques. One way to provide multi-level authentication is embedding the same or different watermarks more than once in the cover media. This type of watermarking can be called as multi watermarking (Wang & Lian, 2012) or embedding more number of watermarks at the same time called multiple watermarks (Takahashi, Nishimura, & Suzuki, 2005). This kind of embedding multiple watermarks or multiple times embedding might increase the robustness of the system against unauthorized claiming, but it may degrade the quality of the cover content. The level of degradation caused due to multiple watermarks embedding can be overcome

* Corresponding author.
E-mail addresses: agila.l@vit.ac.in (A. Loganathan), kganesan@vit.ac.in (G. Kaliyaperumal).

http://dx.doi.org/10.1016/j.eswa.2016.05.019
0957-4174/

by adjusting the pixel values of the cover media in consideration with the human visual characteristics (Hung-Hsu & Chi-Chih, 2011). Since this involves modifying the pixel value directly, it will severely affect the robustness of the watermarking system. Different categories of watermarking systems have been proposed in the last decade. Some of the prominent embedding methods are: additive watermarking (Agilandeeswari, Ganesan, & Muralibabu, 2013; Agilandeeswari, & Ganesan, 2015; Agilandeeswari, & Ganesan, 2016), quantization watermarking (Ng & Garg, 2005), multiplicative watermarking (Peŕez-Gonzaĺez & Mosquera, 2008) and so on. In general the embedding process involves additive watermarking scheme, where the watermark is added with the cover content after multiplying with an embedding factor or the strengthen factor 'α' (Agilandeeswari & Muralibabu, 2013). This embedding factor plays a very important role in controlling the watermark characteristics such as imperceptibility and the robustness of the watermarking system. Higher the embedding factor, higher the robustness and lower the visual quality, whereas, decreasing the embedding factor decreases the level of robustness but improves the visual quality. Efforts have been made to adjust this embedding factor based on the frequency coefficients of the cover content using human visual characteristics (Youssef, ElFarag, & Ghatwary, 2014). This method improves the robustness and imperceptibility, but fails to provide embedding capacity or payload. This problem was addressed by an approach that used the Hop field neural network (Fan & Hongbin, 2005), but it failed to survive against imperceptibility and robustness. Hence, a watermarking system is required that can provide good authenticity by embedding multiple watermarks and also provide better embedding capacity leading to better visual perception and robustness.

This motivates us to introduce a multi-level authentication technique in secure multimedia data transmission for ensuring strict authentication. The main goal of this paper is to design a robust video watermarking system which facilitates secure video transmission over a communication channel by maintaining a trade-off among imperceptibility, robustness and watermark capacity or payload. The proposed Multi-BAM-FUZ video watermarking scheme supports multiple watermarks embedding adaptively using Fuzzy based HVS scheme and Bi-directional associative memory neural networks in wavelet domain. Here, first the multiple watermarks are trained by BAM neural network and then the generated weight matrix is embedded on the cover video both in the luminance and chrominance components using adaptive embedding factors computed by HVS based fuzzy inference system. The embedding is done in uncorrelated mid frequency sub bands of DWT coefficients using PCA.

The proposed Multi-BAM-FUZ scheme addresses various important characteristics of watermarking system such as visual quality or imperceptibility, robustness against all kinds of image processing, geometric and video processing attacks and payload. Thus, it maintains a tradeoff among imperceptibility, robustness and watermark capacity or payload by using hybrid techniques such as BAM Neural network and HVS based Fuzzy inference in wavelet domain.

The rest of the paper is organized as follows. Section 2 describes the related works. Section 3 expresses the review of the existing systems and the contributions of the proposed work. Section 4 discusses the design of the proposed Multi-BAM-FUZ watermarking method. Section 5 gives the experimental results of the proposed method and its comparison with other similar existing methods in Section 6. Conclusions and Future Works are discussed in Section 7.

2. Related works

Cedillo-Hernandez et al. (2014) proposed a robust video watermarking scheme against video transcoding performed on baseband domain. In order to obtain the watermark robustness against video transcoding, four criteria based on Human Visual System (HVS) were employed to embed a sufficiently robust watermark without affecting much its imperceptibility. The quantization index modulation (QIM) algorithm was used to embed and detect the watermark in 2D-Discrete Cosine Transform (2D-DCT) domain. Peak signal to noise ratio (PSNR) and structural similarity index (SSIM) were used to validate the watermark imperceptibility. The experimental results have demonstrated the watermark robustness against video transcoding as well as common signal processing operations and intentional attacks on video sequences. The authors failed to demonstrate the proposed approach in terms of watermark capacity.

A fuzzy-based scheme has been proposed by Youssef et al. (2014) to generate a perceptual membership degree for calculating the strength of the watermark embedding factor. The proposed approach was validated with different benchmark test videos of different sizes, visual characteristics and sampling rates. Several experimental attacks have been applied which includes frame dropping, frame averaging, JPEG compression and Gaussian noises. The method was robust against various geometric and signal processing attacks. The experimental results revealed promising results in terms of visual quality and extracted watermark distortion. But the watermark capacity of the watermarking system has not been discussed. The theoretical framework for the m-QIM video watermarking was proposed by Hasnaoui and Mitrea (2014). The underlying detection method was optimized with respect to minimization of the average error probability, under the hypothesis of white, additive Gaussian behavior for the attacks. This way the data payload was increased by a factor of $\log_2 m$.

Asikuzzaman, Alam, Lambert, and Pickering (2014) have proposed three versions of a blind digital video watermarking algorithm using dual tree complex wavelet transform. The watermark was embedded into the chrominance channel to provide high quality watermarked video. The algorithm was robust against compression, frame averaging, upscaling, rotation and cropping but had limited survival in frame rate conversion and down scaling to an arbitrary resolution. Yassin, Salem, and Adawy (2014) proposed a blind scheme for digital video watermarking. The security of the scheme was established by using one secret key in the retrieval of the watermark. Discrete Wavelet Transform (DWT) was applied on each video frame to decompose it into a number of sub-bands. Maximum entropy blocks were selected and were transformed using Principal Component Analysis (PCA). Quantization Index Modulation (QIM) was used to quantize the maximum coefficient of the PCA blocks of each sub-band. Then, the watermark was embedded into the selected suitable quantizer values. Experimental results showed high imperceptibility. The computed average PSNR exceeded 45 dB. The proposed scheme showed high robustness against several attacks such as JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, and contrast adjustment in test videos. But authors failed to experiment with well-known video processing attacks such as frame dropping, frame averaging, frame resizing and geometrical attack such as rotation. They have not discussed about the watermark capacity.

Ta, Hiep, Tam, and Tanaka (2014) presented a frame-patch matching based robust semi-blind video watermarking using KAZE feature. The KAZE feature is employed for matching the feature points of frame-patch with those of all frames in video for detecting the embedding and extracting regions. The watermark information was embedded in Discrete Cosine Transform (DCT) domain of randomly generated blocks in the matched region. In the extraction process, they synchronized the embedded region from the distorted video by using KAZE feature matching. Based on the matched KAZE feature points, RST (rotation, scaling, and translation) parameters were estimated and the watermark information