Ashdin Publishing
International Journal of Sensor Networks and Data Communications
Vol. 1 (2012), Article ID X110504, 7 pages
doi:10.4303/ijsndc/X110504

Research Article

Performance Analysis of Tracing Watermarking in the *YST* Domain for 3G Video-on-Demand Applications

Francesco Benedetto, Gaetano Giunta, and Antonio Tedeschi

Digital Signal Processing, Multimedia, and Optical Communications Laboratory, Department of Applied Electronics, University of ROMA TRE, via della Vasca Navale 84, 00146 Rome, Italy
Address correspondence to Francesco Benedetto, fbenedet@uniroma3.it

Received 9 May 2011; Revised 9 January 2012; Accepted 10 January 2012

Abstract In the last years, tracing watermarking has been proposed as a technique to provide a blind measure of the quality of service of the communication link, focusing on multimedia communication scenarios. This paper is focused on 3G video-on-demand (VOD) communication scenarios. We have exploited the new color space YST, recently introduced in the literature, where the luminance component (Y) is the same as in conventional YUV space, while the vectors S and T lie within the chrominance (UV) plane. In particular, the third component T, defined as orthogonal to the YS plane, is chosen as the channel for the embedding process (instead of the Y channel). The results show the benefits obtained in digital watermarking by the new representation versus the conventional approach, i.e. the YUV color space. The main contribution of our work is twofold: the sensitivity of the YST representation outperforms the conventional one in terms of both quality (i.e. minimization of the alterations endured by the video during the embedding process) and security issues (i.e. detection of the watermark). Hence, the proposed procedure can be suitably applied for watermarking of 3G video-on-demand applications.

Keywords tracing watermarking; 3G video on demand applications; color image/video processing; quality of service (QoS); multimedia communications

1 Introduction

In recent years, there has been an explosive growth in wireless/mobile networks and obviously an increase demand for platforms with mobile multimedia application support. Hence, multimedia information system security is becoming an issue of increasing importance [2,7,12,13]. As a consequence, the subject of multimedia information system security has attracted intensive research activities in academy, industry and also government. In fact, digital video data can be copied repeatedly without loss of quality. Copyright protection of video data is a more important issue in digital video delivery networks than it was with analog TV broadcast. One method of copyright protection is the addition of a watermark to the video signal which carries information about sender and receiver of the delivered video [20]. Hence, watermarking enables identification and tracing of different copies of video data. Applications are video distribution over the World Wide Web (WWW), pay per view video broadcast, and video on demand services in mobile networks [15,16]. In the mentioned applications, the video data is usually stored in compressed format. Thus, the watermark must be embedded in the compressed domain.

Here, we propose a digital watermarking technique for authentication of multimedia content, e.g. a video on demand (VOD) service. We have implemented a client-server architecture under a Java environment to simulate the real-time VOD service. In particular, we use a novel color space, namely the YST domain, to insert the watermark in the host video. The YST domain was originally presented in [1] with application to still images for quality of service (QoS) assessment purposes. In fact, it aims to minimize the perceptual distortions introduced on the skin color component by a tracing watermarking image processing technique. We extend here the preliminary results of [1], proposing the use of YST as the embedding domain for the authentication of multimedia content. The main contribution of our work is twofold: we show that YST is an efficient embedding domain for the authentication of VOD services and, at the same time, it minimizes the perceptual distortion introduced in the host video during the embedding process.

The remainder of this work is organized as follows. Section 2 describes the materials and methods we have used in this paper. In particular, Section 2.1 presents a briefly overview about related works recently published in order to emphasize what is missing in the current state-of-art. Section 2.2 shows the basic frameworks about the tracing watermarking procedure, while Section 2.3 depicts the basis of the *YST* color domain. Section 2.4 describes the software implementation of the proposed algorithm. Simulation results and discussion are finally presented in Section 3 before our conclusions briefly depicted in Section 4.

2 Materials and methods

2.1 Related works

There are a lot of requirements that must be satisfied by the watermark to be efficiently embedded in the host video. In particular, the major constraints are represented by the following [14]:

- *Payload of the watermark:* this is related with the maximum amount of information that can be stored in a watermark (it depends on the selected application).
- *Watermark granularity:* it represents how much data is needed to embed one unit of watermark information.
- *Robustness:* it measures how robust is the watermark against processing techniques or intentional alterations of the host data.
- *Perceptual transparency:* the watermarking algorithm must embed the watermark such that this does not affect the quality of the underlying host data.

However, a watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the watermarked data or, at least, if the modifications in the watermarked data go unnoticed as long as the data are not compared with the original data. It can be easily understood now that the perceptual transparency of the mark is the major requirement to satisfy during the embedding process. In particular, there are a lot of different embedding techniques at the state of the art that can be used for the following purposes:

- *Copyright protection:* the watermark represents copyright information [6,18].
- *Fingerprinting:* the watermark traces the source of illegal copies [10,22].
- *Copy protection:* the information stored in a watermark can directly control digital recording devices for copy protection purposes [19].
- *Data authentication:* to check the authenticity of the data [5].

Watermarking techniques are not only used for protection purposes. Other applications include:

- *Indexing:* where markers and comments can be inserted in video mail, movies and news items to be used by search engines [17].
- *Medical safety:* embedding the date and the patient's name in medical images could be a useful safety measure [8].
- *Data hiding:* watermarking techniques can be used for the transmission of secret private messages [11].
- *QoS evaluation:* tracing watermarking has been proposed as a technique to provide a blind measure of the quality of service of the communication link [3].

Each of these techniques performs a wide range of modifications in any domain (e.g. spatial domain, Fourier, Wavelet, etc.) and the impact of the modifications can be minimized with the aid of human visual models. Nevertheless modifications can be adapted to the anticipated post-processing techniques or to the compression format of the host data, when the watermark is added to an image in the spatial domain, a pseudorandom noise pattern is added to the luminance values of its pixels. Whereas the conventional watermarking techniques use the luminance and chrominance YUV color space, here we propose to use a novel color space, namely YST. In this way, inserting the mark in the T component (instead of the Y channel) allows to minimize the perceptual distortions (maximizing the perceptual transparency of the mark) introduced by the embedding process, as shown in details in the next sections.

2.2 Tracing watermarking

Spatial spread-spectrum techniques perform the watermarking embedding. In practices, the watermark (narrow band low energy signal) is spread over the image (larger bandwidth signal) so that the watermark energy contribution for each host frequency bins is negligible, which makes the watermark near imperceptible. Following the same methodological approach of [3], a set of uncorrelated pseudo-random noise (PN) matrices (one per each frame and known to the receiver) is multiplied by the reference watermark (one for all the transmission session and known to the receiver): $w_i^{(s)}[k_1,k_2] = w[k_1,k_2] \cdot p_i[k_1,k_2]$, where $w[k_1,k_2]$ is the original watermark, $p_i[k_1,k_2]$ the PN matrices and $w_i^{(s)}[k_1,k_2]$ the spread version of the watermark to be embedded in the ith frame. The embedding is performed in the *DCT* (discrete cosine transform) domain according to the following:

$$F_i^{(w)}[k_1,k_2] = \begin{cases} F[k_1,k_2] + \beta \cdot w_i^{(s)}[k_1,k_2], & (k_1,k_2) \in \Phi, \\ F[k_1,k_2], & \text{otherwise}, \end{cases} \tag{1}$$

where $F_i[k_1,k_2] = DCT\{f_i[k_1,k_2]\}$ is the *DCT* transform of the ith frame; Φ is the region of middle-high frequencies of the image in the *DCT* domain, while β determines the watermark strength and $F_i^{(w)}[k_1,k_2]$ is the *DCT* of the ith watermarked frame. By increasing the value of β, the mark becomes more evident and a visual degradation of the image (or video) occurs. On the contrary, by diminishing its value, the mark can be easily removed by the coder and/or channel's errors. In the application scenario of our simulation trials, the scaling factor β has been chosen in such a way to compromise between the two aforementioned requirements. The ith watermarked frame is then obtained by performing the *IDCT* (inverse *DCT*) of $F_i^{(w)}[k_1,k_2]$, the whole sequence is MPEG-coded and then transmitted through a noisy channel, like shown in the principle scheme of Figure 1.

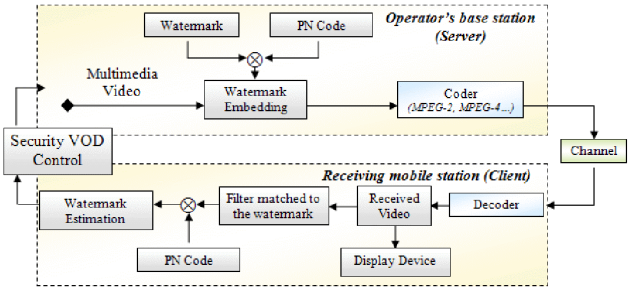

Figure 1: Block scheme of the client-server watermarking technique.

Watermark insertion:

for i=1 to M

{if {(k_1, k_2) ϵ middle-high frequency region}

$$F_i^{(w)}[k_1,k_2] = F[k_1,k_2] + \beta \cdot w_i^{(s)}[k_1,k_2]$$

else

$$F_i^{(w)}[k_1,k_2] = F[k_1,k_2]$$

end;

}

end;

Watermark extraction:

for i=1 to M

{

$$\hat{F}_i^{(w)}[k_1,k_2] = DCT\left\{F_i^{(w)}[k_1,k_2]\right\};$$

$$\hat{w}_i^{(s)}[k_1,k_2] = \hat{F}_i^{(w)}[k_1,k_2] \cdot w[k_1,k_2];$$

$$\hat{w}_i[k_1,k_2] = \hat{w}_i^{(s)}[k_1,k_2] \cdot p_i[k_1,k_2];$$

$$\hat{w}[k_1,k_2] = \frac{1}{M}\sum_{i=1}^{M} \hat{w}_i[k_1,k_2];$$

}

end;

Figure 2: Pseudo-code of the embedding/extraction procedure.

The receiver implements video decoding as well as watermark detection, see Figures 1, 2, and 3. Moreover, Figure 2 depicts here the pseudo-code of the of the embedding/extraction procedure, in order to help readers following the insertion and extraction processes, while Figure 3 shows the block scheme of the whole embedding/extraction procedure. More in details, at the same time after decoding of the video-stream, a matched filter extracts the (known) watermark from the DCT of each nth received I-frame of the sequence. The estimated watermark is matched to the reference one (despread with the known PN matrix). The matched filter is tuned to the particular embedding procedure, so that it can be matched only to the randomly spread watermark. It is assumed that the receiver knows the initial spatial application point of the mark in the DCT domain.

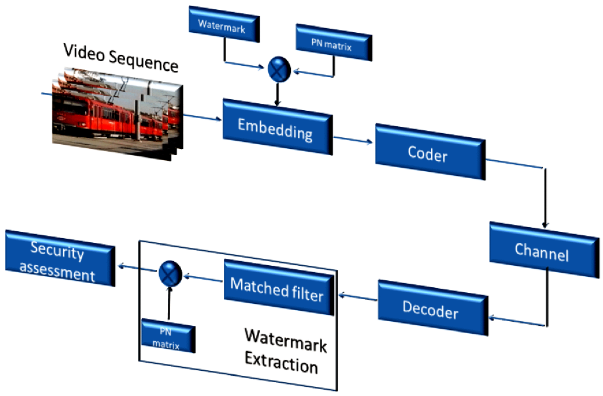

Figure 3: Block scheme of the whole embedding/extraction procedure.

Each received frame undergoes the DCT transform $\hat{F}_i^{(w)}[k_1,k_2] = DCT\{F_i^{(w)}[k_1,k_2]\}$ and the middle-high frequency region of embedding is selected. Now, the corresponding portion the transformed frame is multiplied by the watermark, which is known at the receiving side, thus obtaining an estimation of the spread version of the watermark embedded in the ith frame $\hat{w}_i^{(s)}[k_1,k_2] = \hat{F}_i^{(w)}[k_1,k_2] \cdot w[k_1,k_2]$. Finally, the dispreading operation, for the generic ith frame, is then performed multiplying the spread version of the received ith watermark with the corresponding PN matrix: $\hat{w}_i[k_1,k_2] = \hat{w}_i^{(s)}[k_1,k_2] \cdot p_i[k_1,k_2]$. The watermark is then estimated by averaging the dispread watermarks (one for each watermarked frame) over the M transmitted frames: $\hat{w}[k_1,k_2] = \frac{1}{M}\sum_{i=1}^{M} \hat{w}_i[k_1,k_2]$. A possible index of the degradation is simply obtained by calculating the mean of the error energy (i.e. its mean-square-error, MSE) as follows:

$$MSE = \frac{1}{M}\sum_{n=1}^{M}\left(\sum_{k_1=1}^{K_1}\sum_{k_2=1}^{K_2}\left(w_n[k_1,k_2] - \hat{w}_n[k_1,k_2]\right)^2\right), \quad (2)$$

where $w_n[k_1,k_2]$ and $\hat{w}_n[k_1,k_2]$ represent the original and the extract watermark respectively, and $n = 1,\ldots,M$ is the current frame index. However, since the watermarked video may undergo different kinds of attacks during the download, we are here interested in obtaining another index, indicating the robustness of the proposed approach: at the receiving side the watermark message is detected using a correlation coefficient (compared against some threshold value) between the original watermark and the attacked video. The correlation coefficient is defined as follows:

$$\rho = \frac{\sum_{k_1=1}^{K_1}\sum_{k_2=1}^{K_2} w_n[k_1,k_2] \cdot \hat{w}_n[k_1,k_2]}{\sqrt{\sum_{k_1=1}^{K_1}\sum_{k_2=1}^{K_2} w_n^2[k_1,k_2]} \cdot \sqrt{\sum_{k_1=1}^{K_1}\sum_{k_2=1}^{K_2} \hat{w}_n^2[k_1,k_2]}}. \quad (3)$$

2.3 The YST color space

An image can be presented in a number of different color space models [4]. *RGB* stands for the three primary colors: red, green, and blue, it is a hardware-oriented model and is well known for its color-monitor display purpose. The main idea in usual methods is to transform *RGB* signal to make brightness explicit so that it can be discarded. Only chromatic information is kept and used for the adopted image processing technique. The choice of the color space can be a very important decision which can dramatically influence the results of the processing. The knowledge of various color spaces can ease the choice of the appropriate color space. The *RGB* color space is good for image display but is not the best when analyzing images using the computer. In fact, one of the problems of the *RGB* color space is its perceptual non-uniformity, i.e. its low correlation between the perceived difference of two colors and the Euclidian distance in the *RGB* space.

Moreover, the main disadvantage of the *RGB* color space in applications with natural images is a high correlation between its components: a value of about 0.78 for the cross-correlation between the B and R channel, a value of 0.98 and 0.94, respectively, for the correlation between R and G and between G and B [21]. Because of this high correlation between the channels, the *RGB* domain is, hence, not suitable for image processing techniques, such as digital watermarking applications [9]. The potential of these three channels can be exploited for the application of watermarking, by decreasing the correlation among them. Other colors systems exist which have the property of separating the luminance component from chromatic component and with that at least partial independence of chromaticity and luminance is achieved. Such color spaces are for example *YCbCr* and *YUV*, where Y stands for "luminance" and represents the brightness, while Cr, Cb, U and V represent the chrominance components, providing color information and are "color difference" signals of blue minus luminance ($B-Y$) and red minus luminance ($R-Y$), respectively. In practices, an image can be presented in a number of different color space models such as [4]:

- *RGB* (as said before) stands for the three primary colors: red, green, and blue. It is a hardware-oriented model and is well known for its color-monitor display purpose;
- *YCbCr* is another hardware-oriented model. However, unlike the RGB space, here the luminance is separated from the chrominance data;
- *HSV* is an acronym for hue-saturation-value. Hue is a color attribute that describes a pure color, while saturation defines the relative purity or the amount of white light mixed with a hue; value refers to the brightness of the image. This model is commonly use for image analysis but it is not suitable for video coding.

These are some, but certainly not all, of the color space models available in image processing.

Recently, a novel color space, namely *YST*, has been proposed in [1] to model the human skin in order to minimize the perceptual distortions introduced on the skin color component by image processing techniques, such as digital watermarking. In particular, the new color space must satisfy the following conditions: the luminance must be the same of the *YUV* color space because Y is the component used in MPEG-4 for motion-compensation and must remain unaltered; one component, S, must be ad hoc created to match the vector corresponding to the skin color and finally, the conversion to and from this new color space must be reversible. In practice, the vector S lays in the plane identified by the chrominance components U and V, i.e. it is a linear combination of only these two components. In this way, the vector S represents the mean value of the human "skin," in the sense that it stands for the average chrominance component of the human skin. It has to be noted that in [1] the vector S is characterized by unitary modulus (i.e. S is a versor). This means that S represents the direction of the average chrominance component of the human skin. In other words, the vector S corresponds to infinite human skin with different tones of luminance given by the combination of S with the luminance Y. This means that the chrominance of the skin remains nearly the same for different kind of people (i.e. different genders) while the luminance changes, from white to black, corresponding to different linear combinations of S and Y. Finally, the vector T is automatically identified in order to have a component that is orthogonal to the plane spanned by the other two vectors Y and S. It is interesting to point out that in the novel color space *YST*, as well as in *YUV*, the luminance component is decoupled from the color information of the image. As a consequence, the skin-color model can remain effective regardless of the variation of skin color (e.g., black, white, or yellow) because the derivation of the model is independent of the luminance information of the image, as already stated in [4].

2.4 Proposed approach

Video on Demand (VOD) or Audio and Video on Demand (AVOD) are systems which allow users to select and watch/listen to video or audio content on demand. IPTV technology is often used to bring video on demand to televisions and personal computers. Television VOD systems either stream content through a set-top box, a computer or other device, allowing viewing in real time, or download it to a device such as a computer, digital video recorder (also called a personal video recorder) or portable media player for viewing at any time. A client-server is a software architecture model consisting of two parts, client systems and server systems, both communicate over a computer network.

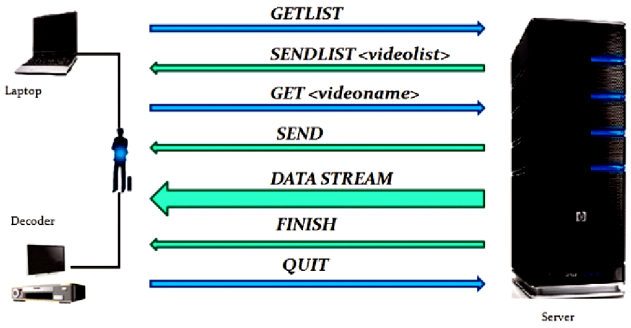

Figure 4: Client-server protocol messages.

A client-server protocol is a protocol in which there is a single server which listens for connections, usually on a specific port (if this is TCP, UDP, or a similar protocol), and one or more clients which connect to it. All of the machines that access the server are called clients or workstations. The rules regarding the communication between the client and the server (i.e. the communication protocol) are of fundamental importance. Referring to Figure 4, we have implemented the following protocol to simulate the VOD service in order to analyze the performance of the watermarking procedure in the *YST* domain, in real-time conditions.

In particular, and following the JAVA methodology approach, we have defined the following:

- GETLIST: allows the client, to obtain the video list from the server;
- SENDLIST: allows the server to send the list of currently available videos;
- GET: it allows the client to select the video that the server will send;
- SEND: it allows the server to send the video data (i.e. DATA STREAM) after the embedding process is completed;
- FINISH: it allows the server to notify to the client that the video has been completely transmitted;
- QUIT: allows the client to close the connection with the server.

3 Results and discussion

In this Section, some experimental results characterizing the effectiveness of the proposed method for secure video on demand download are presented. We have simulated the video on demand service and the client server architecture under a JAVA environment, as explained in Figure 4 and detailed in the previous section. At the beginning of the VOD service, the client (i.e. the user's mobile equipment, decoder or laptop) first connects to the server (i.e. the operator's multimedia center or base station), and then requests the list of the available videos. Subsequently, the client starts the video downloading and checks the data integrity with the watermarking technique previously described. The dimensions of the video-sequences employed in our experimentations have been properly chosen in order to simulate a multimedia service in a UMTS scenario. Therefore, QCIF (144×176) video sequences, which well match the limited dimensions of a mobile terminal's display, have been employed and a frame rate of 15 fps has been chosen. We have analyzed, through a comparative analysis the embedding procedure implemented in the YST color space with the same embedding procedure implemented using the conventional YUV domain. The rationale behind our choice (i.e. the grounds for comparison) has been carried out in order to let readers know that our choice is deliberate and meaningful, not random. In fact, we are here comparing the same embedding (i.e. the tracing watermarking) using the novel color space (YST) and the conventional, at the state-of-art, domain (YUV).

In particular, whereas for the YST domain the watermark has been inserted in the T channel in order to minimize the perceptual degradation in the video caused by the embedding process, the conventional technique embeds the mark in the luminance component (i.e. Y). In this way, we can compare and analyze the performance of the two methods using the classic compare-and-contrast approach: we weight YST and YUV equally, underlining that they have similar properties but crucial differences as well, finally turning out that they have completely different performances. The marked video is then transmitted over noisy channels, simulated by Poisson's generators of random transmission errors. Specifically, wireless channels characterized by different levels of bit error rate (BER) have been designed (from 10^{-5} to 10^{-3}). In all the following simulations, we have used the common test video-sequences (such as *Carphone*, *Foreman*, *Miss America*, and *Suzie*), all MPEG-4 coded and considered for different kinds of attacks (e.g. cropping, resizing, and rotating).

Figure 5 shows here the correlation coefficient (left) and the MSE (right) of the watermark after a cropping attack. As it can be easily seen by the graphs, the curve referring to the correlation coefficient of the watermark embedded in the *YST* domain is always higher than the other curve (that refers to the correlation coefficient of the watermark embedded in the *YUV* domain). This means that the *YST* color space is a more efficient embedding domain for digital watermarking of multimedia data. Conversely, the curves referring to the MSE of the watermark, see Figure 5(b), shows that the *YST* domain minimize the alteration endured by the watermarking process in the host video. The curve referring to the *YST* domain is always lower that the one referring to the *YUV* color space.

The same happens for both the resizing (see Figure 6) and rotating (see Figure 7) attack. Again, the *YST* color

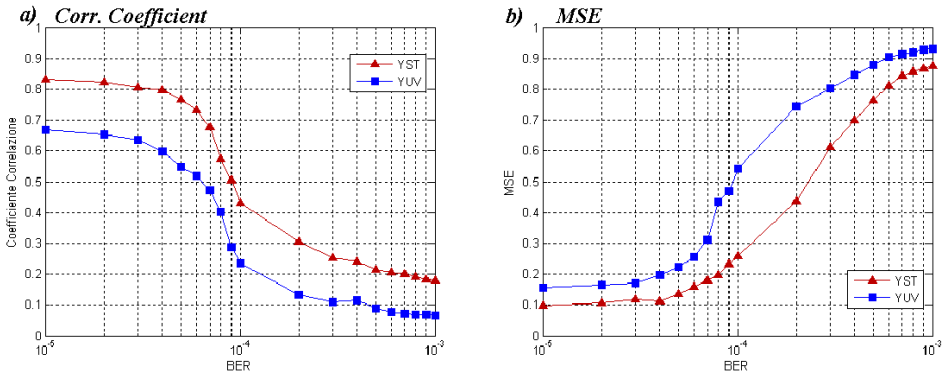

Figure 5: *Cropping* attack: (a) Correlation Coefficient and (b) normalized MSE versus different BER of interest.

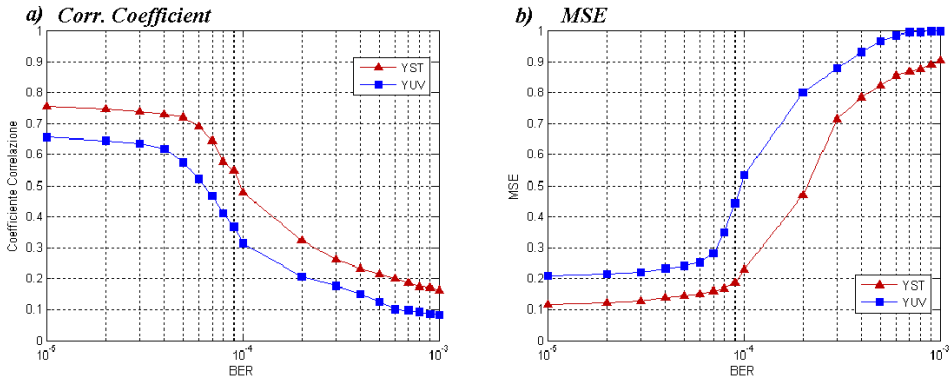

Figure 6: *Resizing* attack: (a) Correlation Coefficient and (b) normalized MSE versus different BER of interest.

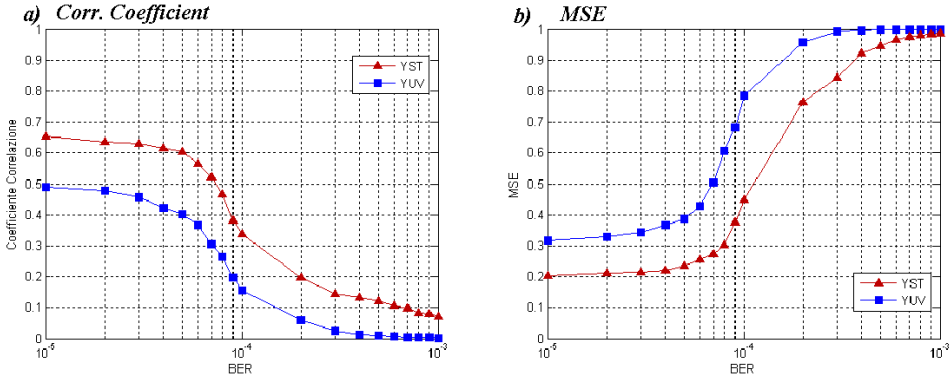

Figure 7: *Rotating* attack: (a) Correlation Coefficient and (b) normalized MSE versus different BER of interest.

space reveals to be the most efficient domain for the watermark embedding: we have a probability of watermark detection that is greater in the *YST* domain (since the correlation coefficient is higher in this color space) than in the *YUV* domain. At the same time, it also minimizes the alterations endured by the host video data. The obtained results show the capability of this watermarking technique of multimedia content to trace the attacks suffered by the videos downloaded through the network, minimizing at the same the alterations endured by the host video during the embedding process. Moreover, our simulation trials have evidence the benefits of the new color representation for digital watermarking application instead of using the conventional approach (inserting the mark in the luminance component). We have verified that realizing the watermark embedding in the new color space YST (specifically, inserting the mark in T) minimizes the degradations suffered by the video during the processing and allows

a better detection of the watermark as well. In particular, such method can be usefully employed for a number of different authentication purposes in wireless multimedia communication networks such as: control feedback to the sending user about the data integrity; detailed information to the operator about the security of the communication link.

4 Conclusions

In this paper, we have investigated the use of the new color space *YST* to perform authentication of multimedia content by tracing watermarking, minimizing the distortions introduced by the embedding process. The simulation outcomes show the benefits obtained in digital watermarking by the new representation: the sensitivity of the *YST* representation outperforms the conventional one in terms of both correlation coefficient (i.e. detection of the watermark) and MSE (i.e. minimization of the alterations endured by the host video). Hence, the proposed procedure can be suitable applied for authentication of video on demand services.

References

[1] F. Benedetto, G. Giunta, and A. Neri, *A new color space domain for digital watermarking in multimedia applications*, in IEEE International Conference on Image Processing (ICIP '05), vol. 1, Genova, Italy, 2005, 249–252.

[2] C. Busch, W. Funk, and S. Wolthusen, *Digital watermarking: from concepts to real-time video applications*, Computer Graphics and Applications, IEEE, 19 (1999), 25–35.

[3] P. Campisi, M. Carli, G. Giunta, and A. Neri, *Blind quality assessment system for multimedia communications using tracing watermarking*, IEEE Transactions on Signal Processing, 51 (2003), 996–1002.

[4] D. Chai and K. N. Ngan, *Face segmentation using skin-color map in videophone applications*, IEEE Transactions on Circuits and Systems for Video Technology, 9 (1999), 551–564.

[5] C. Fei, R. H. Kwong, and D. Kundur, *A hypothesis testing approach to semifragile watermark-based authentication*, IEEE Transactions on Information Forensics and Security, 4 (2009), 179–192.

[6] X. Feng, H. Zhang, H.-C. Wu, and Y. Wu, *A new approach for optimal multiple watermarks injection*, Signal Processing Letters, IEEE, 18 (2011), 575–578.

[7] F. Frattolillo, *Watermarking protocol for web context*, IEEE Transactions on Information Forensics and Security, 2 (2007), 350–363.

[8] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, *Multiple image watermarking applied to health information management*, IEEE Transactions on Information Technology in Biomedicine, 10 (2006), 722–732.

[9] S. A. M. Gilani, I. Kostopoulos, and A. N. Skodras, *Color image-adaptive watermarking*, in 14th International Conference on Digital Signal Processing (DSP '02), vol. 2, 2002, 721–724.

[10] N. S. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, *Extrinsic channel-like fingerprinting overlays using subspace embedding*, IEEE Transactions on Information Forensics and Security, 6 (2011), 1355–1369.

[11] J.-M. Guo and J.-J. Tsai, *Data-hiding in halftone images using adaptive noise-balanced error diffusion*, Multimedia, IEEE, 18 (2011), 48–59.

[12] F. Hartung and M. Kutter, *Multimedia watermarking techniques*, Proceedings of the IEEE, 87 (1999), 1079–1107.

[13] F. Hartung and F. Ramme, *Digital rights management and watermarking of multimedia content for m-commerce applications*, Communications Magazine, IEEE, 38 (2000), 78–84.

[14] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, *Watermarking digital image and video data. A state-of-the-art overview*, Signal Processing Magazine, IEEE, 17 (2000), 20–46.

[15] S.-Y. Lee, G.-Y. Cho, and J.-N. Kim, *The recording method of real time DMB encryption for PMP*, in Second International Conference on Future Generation Communication and Networking Symposia (FGCNS '08), vol. 3, Sanya, Hainan Island, China, 2008, 218–221.

[16] B. Mathieu, P. Paris, G. Le Guelvouit, and S. Rouibia, *A secure and legal network-aware P2P VoD system*, in Fifth International Conference on Internet and Web Applications and Services (ICIW '10), Barcelona, 2010, 194–199.

[17] A. Qamra, Y. Meng, and E. Y. Chang, *Enhanced perceptual distance functions and indexing for image replica recognition*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 27 (2005), 379–391.

[18] A. Rial, J. Balasch, and B. Preneel, *A privacy-preserving buyerseller watermarking protocol based on priced oblivious transfer*, IEEE Transactions on Information Forensics and Security, 6 (2011), 202–212.

[19] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, *A provably secure anonymous buyerseller watermarking protocol*, IEEE Transactions on Information Forensics and Security, 5 (2010), 920–931.

[20] R. Samtani, *Ongoing innovation in digital watermarking*, Computer, 42 (2009), 92–94.

[21] M. Tkalcic and J. F. Tasic, *Colour spaces: perceptual, historical and applicational background*, in International Conference on Computer as a Tool (EUROCON '03), vol. 1, 2003, 304–308.

[22] M. Wu, W. Trappe, Z. J. Wang, and K. J. R. Liu, *Collusion-resistant fingerprinting for multimedia*, Signal Processing Magazine, IEEE, 21 (2004), 15–27.