

WATERMARKING PROTECTION FOR 3D IMAGES

Marius ROGOBETE¹

Ciprian RACUCIU²

¹ Eng. PhD, GE Alstom Alliance, Bucharest, Romania

² Prof. Eng. PhD Titu Maiorescu University, Bucharest, Romania

Abstract: *The 3D digital contents are increasing rapidly on the media market and games market but the techniques of copyright protection are still on the low level. The existing watermarking 3D models focused on the robustness against possible attacks to destroy the embedded watermarks, are using to hide copyright information. But a clear auto-protection able to embed a visible 3D watermarks into the original 3D image, but also capable to remove the watermark without 3D host image damage, is not yet presented in the specific scientific literature. Our proposed algorithm overlaps a removable watermark image over the 3D host, original image. It could be removed based on several parameters encrypted in a hide watermark. A 3D watermark is hiding, using surface curvatures, by segmentation of the regions over the given 3D triangular mesh. The watermark is embedded to the areas by statistically modulating the distance between each mesh vertex and the mass center of the mesh. The presented algorithm embeds a visible watermark in a 3D host image together with a hide encrypted message on the sender side and then, on the receiver side, extracts the parameters and decrypts them, in order to remove the visual watermark.*

Keywords: 3D images, visual watermark protection, copyright protection, hide watermark

INTRODUCTION

State of the art

The protection of digital 3D image models is actually using two kinds of methods:

- A 3D hiding watermarking is embedded into 3D model data, in this way the presence of the watermark verifies the copyright;
- Most used method is the metadata structure, that is a segment of data attached to the image, and summarizes basic information about image but also more data providing tracking information, as is author, data of creation/acquisition, location and standard used [2][10][11][12].

Every method covered specific area of protection, as the hide watermark allows the data protection verification when the owner has access to the copied 3D image, the metadata contains any kind of data including copyright info, it could be relatively easy removed, e.g. using a hexadecimal editor.

In conclusion, there are several important disadvantages of the 3D image protection methods, which permit to any user to use copies of the images or of the frames streams without warnings.

What is new

This work is developing an algorithm and method able to warn any user about the copyright. This process is possible as a visual watermark is embedded into 3D image. The watermark image is overlapping the original image in such a way that the original image is not damaged but also the watermark image is visible, therefore, the looker will see the watermark message (a logo or a clear copyright message).

Protection and permission

The 3D protection is solved as the visual watermark is covered the host 3D image, and it appears over the still image or even over every 3D frame of a video stream. But how it works when a user has whole permission to use the image or video stream?

Our method is able to remove the embedded watermark from the watermarked image, in order to have the original image, when the user has specific browser plug-in or framework. This

algorithm and process is described in the present article.

METHOD DESCRIPTION

The research is based on [1][3] and [5]. Using an image with explicit message of copyright as visual watermark embedded into original image, results a watermarked image that contains a clear message regarding the owner of the photo and/or copyright. In order to remove the embedded watermark that overlaid the original image, it is necessary to use an embedding function that could be invertible [6]. This is possible when the embedding process of the watermark into the host image is done with a bijective function $f()$, and for the inverse process (to remove the visual watermark) is used the inverse function $f^{-1}()$. The bijective function should have also several characteristics that make the inserted visual watermark sufficient transparent to don't disturb

the original image information, but to have a good visibility over the host image [9].

Functional blocks

The method has two main modules (figure 1), the sender and receiver. The sender is the part where the owner is protecting the produced images, adding a visual watermark over the host image.

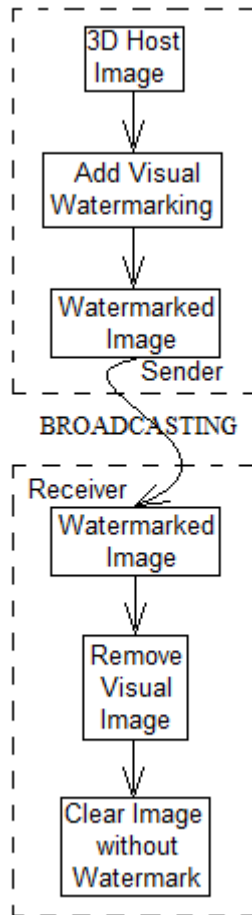


Figure 1. Sender/Receiver 3D Image Watermarking Process

The receiver module captures the watermarked 3D image broadcasted by the owner and is trying to remove the watermark image and the obtain a compensated image as close as possible of the original, host image.

Sender module

The sender block functions (figure 2) are hidden the embedding function parameters into a hide watermark, therefore the parameters to be extracted by the receiver. Using an bijective embedding function based on these parameters, the visual watermark is embedded into the host image. It results a watermarked image with the watermark image overlaps the host, original image.

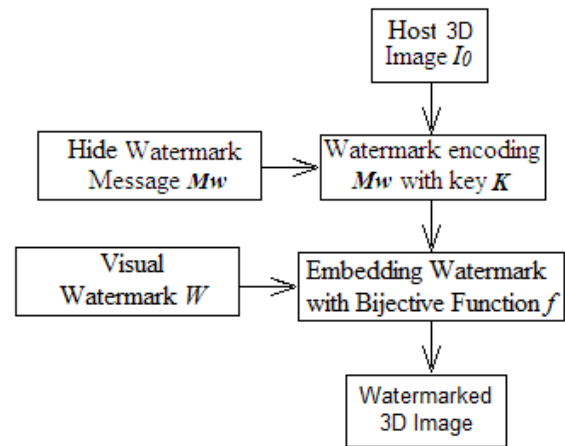


Figure 2. Sender module's blocks

Receiver module

On the receiver side, when the protected 3D image is received, the framework is trying to apply the inverse embedding function f^{-1} in order to compensate the embedded visual watermark (figure).

If the receiver can apply the key K then the license is recognized and thus, using specific parameters extracted from the hide watermark, the inverse function will compensate the embedded image.

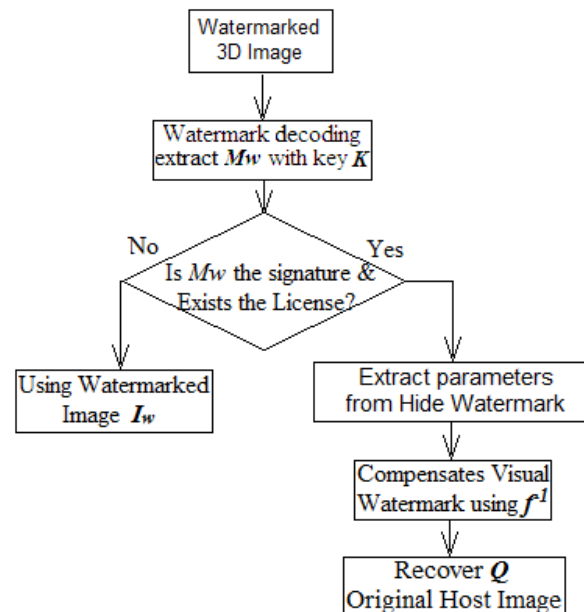


Figure 3. Receiver module & main functional blocks.

Visual Watermark - embedding process

The visual watermark embedding process is using specific bijective function of the form (1). It is applied on the host image over the common pixels with the visual watermark image.

Thus, into the host image I_0 (figure 3) is embedded the visual watermark image W using a function of general form (1) [8] [9]:

$$\forall i_{0_{n,m}} \mid i_{0_{n,m}} \in \{I_0 \cap W\} \Rightarrow i_{w_{n,m}} \Rightarrow \begin{cases} R = cR + \frac{iR_{0_{n,m}} * (vR_{max} - vR_{min})}{255} \\ G = cG + \frac{iG_{0_{n,m}} * (vG_{max} - vG_{min})}{255} \\ B = cB + \frac{iB_{0_{n,m}} * (vB_{max} - vB_{min})}{255} \end{cases} \quad (1)$$

, where vR_{min} , vG_{min} and vB_{min} are minimum values on the channel band and vR_{max} , vG_{max} and vB_{max} are maximum values, choose by the user. The low limits of the colors of inserted image are cR , cG and cB .

Having the I_0 host image of $N \times M$ size and the watermark image W of the same $N \times M$ size with d as an arbitrary constant value, the results IW is the image with watermark embedded using the embedding function (2) [9]:

$$i_{w_{n,m}} = \begin{cases} f(i_{0_{n,m}}) & \text{for } w_{n,m} = 0 \\ i_{0_{n,m}} & \text{for } w_{n,m} = 1 \end{cases} \quad (2)$$

The invers function, f^{-1} allows completely compensate the embedded watermark and to recover the original host image without lossing quality. Having the recovered image Q , the mathematical form(3) is [6]:

$$q_{n,m} = \begin{cases} f^{-1}(i_{w_{n,m}}) & \text{for } w_{n,m} = 1 \\ i_{w_{n,m}} & \text{for } w_{n,m} = 0 \end{cases} \quad (3)$$

The resulted recovered image Q has the same $N \times M$ size as original host image.

CONCLUSIONS

Using similar 2D visual watermark schema for copyright, but correlated with 3D hidden watermark algorithm we developed a method able to protect 3D image with coherent visible warning on the still or dynamic image frame.

Any block of the sender/receiver schematics were tested separately but, for this specific approach, we need to implement the whole application in order to compare the functional behavior, as future work.

Embedding hidden Watermark

The hidden watermarking into 3D models has specific characteristics as the 3D models are represented in most of cases because 3D triangular meshes [13], [14]. The presented method is based on S. Nakazawa research [13] being a blind watermarking method using visual principal elements area correlated with the input 3D meshes.

The first step is to identify the visual prominent shape of 3D mesh, being in fact a comparison between the neighborhood and the specific vertex (4).

$$Cv(v_i) = \frac{1}{2S} \sum_{k=0}^{Ni} (\cot \omega_{i,k} + \cot \delta_{i,k})(x_i - x_k) \quad (4)$$

Where Cv is the curvature at the vertex v_i , Ni is a set of vertices in the immediate neighborhood of the v_i , and S is the area surrounded the curvature at the vertex.

Practically it is used a Gaussian function F that searches the neighboring vertices x in a radius of $2r$ of v and computes the weighted average of mean curvature:

$$F(Cv(v_i), r) = \frac{\sum_{k=Nv}^{N2r} (Cv(x) \exp[-\|x - v\|^2 / 2r^2])}{\sum_{k=Nv}^{N2r} \exp[-\|x - v\|^2 / 2r^2]} \quad (5)$$

Where Nv and $N2r$ are the neighborhood vertices around v . Finally, the prominent mesh of the vertices assigned to v is the Gaussians difference (6):

$$Pr(v) = |F(Cv, r) - F(Cv, 2r)|. \quad (6)$$

The hidden watermark is embedding into every bit of the normalized vertex, calculated as the distance from the barycenter of the 3D mesh [13]. The watermark extraction is a similar process, where the prominent regions of the watermarked 3D mesh are identified based on the histogram of the vertex norms. The variance comparison of each divided bin detects the corresponding embedded watermark bit.

BIBLIOGRAPHY

- [1] Rogobete, M. – First and second order image statistics in specific image artifact detection, International Conference of Innovative Technologies, September 26 - 29, 2012, Croatia
- [2] Rogobete, M., Răcuciu, C. - A Watermarking Framework for Image Protection. A case study, Symposium on Automated Systems and Technologies, St. Petersburg, Russia, May 2015
- [3] Rogobete, M., Răcuciu, C. – Using Potential Field Analysis into Image Artifact Detection Field, Indian Journal of Research, Volume III, Issue V, May 2014
- [4] Rogobete, M.; Răcuciu, C. – Original methodology and algorithm able to identify visible noisy in still images and video stream, MegaByte Journal of Titu Maiorescu University, no.12/2012, Bucharest, 2012
- [5] Rogobete, M.; Răcuciu, C.; Apostol, C.G.; Pîrloagă, D.M. – An OOP method to update the digital watermarking application during running time, The International Conference NAV-MAR-EDU 2013, Constanța 2013
- [6] Rogobete, M.; Răcuciu, C. - An Improved Cryptographic Method in Watermark Encoding , Indian Journal of Research, Volume IV, Issue III, March 2015
- [7] Rogobete, M.; Răcuciu, C. - Cryptographic Extension Key for Watermark Encoding, Titu Maiorescu – 04.11.2014, International Conference for Education and Creativity, Bucharest, Romania
- [8] Rogobete, M.; Răcuciu, C.; Pîrloagă, D.M.; Medeleanu, F. – Using Hide Watermark in Visual Watermark extraction. Advantages. Algorithm, SEA-CONF2015, May 2015, Constanța, Romania
- [9] Rogobete, M.; Răcuciu, C. - Visual Watermark Embedded Functions, Titu Maiorescu – 04.11.2014, International Conference for Education and Creativity, Bucharest, Romania
- [10] Rogobete, M.; Răcuciu, C. - O nouă abordare practică în protecția imaginilor digitale, Conferința "Cercetări doctorale în domeniul afacerilor interne", Academia de Poliție, București, Iunie 2015
- [11] Rogobete, M.; Răcuciu, C.; Pîrloagă, D.M. -, Medeleanu, F.; – Using Hide Watermark in Visual Watermark extraction.. Advantages. Algorithm, “Mircea cel Batran” Naval Academy Scientific Bulletin, Volume XVIII, 2015, Issue 1, pg. 366-368
- [12] Rogobete, M.; Răcuciu, C.; Pîrloagă, D.M.; Medeleanu, F. – Image Protection. A Framework Proposal, SEA-CONF2015, May 2015, Constanța, Romania
- [13] Nakazawa S, Kasahara S, Takahashi S, "A Visually-Enhanced Approach to Watermarking 3D Models", Japan Society of the Promotion of Science, Oct. 2010, IEEE Transactions
- [14] Liu, Y.; Prabhakaran, B.; Guo, X. "Blind invisible watermarking for 3D meshes with textures", 2010 IEEE International Conference on Image Processing, 26-29 Sept. 2010, IEEE Transactions, pages: 3689 - 3692