**"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 2**
**Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:**
**PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace**

# IMAGE PROTECTION A FRAMEWORK PROPOSAL

**Marius ROGOBETE**[1]
**Ciprian RACUCIU**[2]
**Marian-Dorin PIRLOAGA**[3]
**Florin MEDELEANU**[4]
[1] Eng. Alstom GRID Bucharest, Romania
[2] Prof. eng. PhD, "Titu Maiorescu" University, Bucharest, Romania
[3] Inf. Military Technical Academy, Bucharest, Romania
[4] Eng. Military Technical Academy, Bucharest, Romania

***Abstract:*** *Actually the image protection is based on the attached information to the main image information and presented as a container. Any player or browser uses plugins that extract the image in order to be properly played. But also it allows that the image to be saved separately, without additional info attached. More, basically all the pictures in Facebook or Twitter are detached by the extra information. Therefore the only way to keep the info into any image is to embed it, as the watermarking technology describe. Based on former research, here is presented a specific framework able to protect pictures and images stream.*

INTRODUCTION

For an efficient copyright protection of photos, video stream's frames or any other kind of digital images, a safe method is to stamp the original image with a logo image. The watermark image that overloads the host image should befixed theoretically without removing possibility, like the classical method of visual embedding watermark.

Using this property, an image creator or copyright holder can embed visible and hide watermarks into image, using a specific framework.It is using a non-reversible embedding watermark function when the image/video stream is distributed without control in order to avoid any attack.

When a reversible function is used then the watermark is removable and the framework couldallow the receiver far end to eliminate the visible watermark based on the invers embedding function. In this way, only the controlled receivers could profit by the clean photos/video stream.

The hide watermark could embed typical information that identifies the owner and, more important, transfers parameters for inverse embedding function.

When the framework's receptor module tries to eliminate visible watermark, it checks, first of all, the owner info embedded with hide watermark. If the hide information integrity is damaged (the frame/photo was changed) then the removing process is not done.

EMBEDDING FUNCTION

The non-reversible function has the general form (1).

$$\forall q_{0_{n,m}} \Big| q_{0_{n,m}} \in \{Q_0 \cap W\} \Rightarrow$$
$$\Rightarrow i_{w_{n,m}} = \begin{cases} R = cR + \dfrac{qR_{0_{n,m}} * (vR_{\max} - vR_{\min})}{255} \\ G = cG + \dfrac{qG_{0_{n,m}} * (vG_{\max} - vG_{\min})}{255} \\ B = cB + \dfrac{qB_{0_{n,m}} * (vB_{\max} - vB_{\min})}{255} \end{cases} \quad (1)$$

, where $R_{min}$, $G_{min}$ and $B_{min}$ are minimum values on the channel band and $R_{max}$, $G_{max}$ i $B_{max}$ are maximum values, choose by the user. The low limits of the colors of inserted image are *cR, cG* and *cB*.

The bijective (reversible) function form (2) is:

$$\forall q_{0_{n,m}} \Big| q_{0_{n,m}} \in \{Q_0 \cap W\} \Rightarrow$$
$$\Rightarrow q_{w_{n,m}} = \begin{cases} q_{0_{n,m}} + d, \; for \quad q_{W_{n,m}} \in (0,255) \\ (q_{0_{n,m}} + d) \bmod 256, \; for \quad q_{W_{n,m}} \notin (0,255)] \end{cases} \quad (2)$$

where $q_{w_{n,m}} \in Q_W, \quad n = 0,...,N-1, \quad m = 0,...,M-1, \quad d \in Z.$

And an example of general numeric algorithm for reversible function $f(q_{w_{n,m}}) = r_{0_{n,m}} + d$ is (3) [9]:

$$q_{w_{n,m}} = \begin{cases} f(q_{0_{n,m}}) \quad for \quad w_{n,m} = 0 \\ q_{0_{n,m}} \quad for \quad w_{n,m} = 1 \end{cases} \quad (3)$$

The invers function, $f^{-1}$ allows completely compensate the embedded watermark and to recover the original host image without losing quality. Having the recovered image *R*, the mathematical form is [9]:

$$r_{n,m} = \begin{cases} f^{-1}(q_{w_{n,m}}) \quad for \quad w_{n,m} = 1 \\ q_{w_{n,m}} \quad for \quad w_{n,m} = 0 \end{cases} \quad (4)$$

FRAMEWORK PRESENTATION

As the entire watermark properties are directly set by theembedding functions, when the embedding function is bijective, the recovered image is identical with the original host image if the inverse function is applied [6].

The embedding and, when is decide, the extracting process ofa visual watermark into/from any host image is executed using aframework. The bijective function is applied whether the sender decides to remove the visual watermark from image on the receiver side, or non-bijective one if no receiver is allowed to secure the clean image. A visual watermark or identification logo (figure 1) is an image that overlays the host image (figure 2). The output watermarked image is distributed over media, using communication devices/channels, usually without any receiving control.

**Figure 1. The watermarking image**

**Figure 2. The host image**

On the receiver side, the watermarked image or even video stream sequence could be usedas it is, with the image watermark embedded (figure 3).

**Figure 3. The watermarked image**

In this case, the framework doesn't use the inverse embedding function on the receiver side.

The receivers, who have specific plugins installed in the browser, will try to extract the watermark, in order to recover the original image [2]. When the embedding watermark process is reversible (the embedding function is bijective), a complete extraction is possible using specific inverse embedding function. The framework supplies the inverse watermark embedding function, in order to recover the original image.

Whether the receiver is not licensed/not recognized or the image is modified (the hide watermark is not identified) then the visual watermark is not extracted or it is incomplete eliminated [3] [4]. In this way the image integrity is checked (the signature from the hidden watermark), and the visual copyright protection is removed if the original image was not tampered.

FRAMEWORK FUNCTIONALITIES

On the owner side (figure 4), a semi-robust watermark message *Mw* is hidden into the host image using LSB method (for a simple implementation but could be used also a cryptographic algorithm [5] [7]). The hidden message contains two data:

- The owner identification string (*Sid*)
- A constant parameter, *d* in equation (3), of 8 bytes size, used in the inverse function

Also a stego image is embedded, for the geometrical locus of visual watermark.

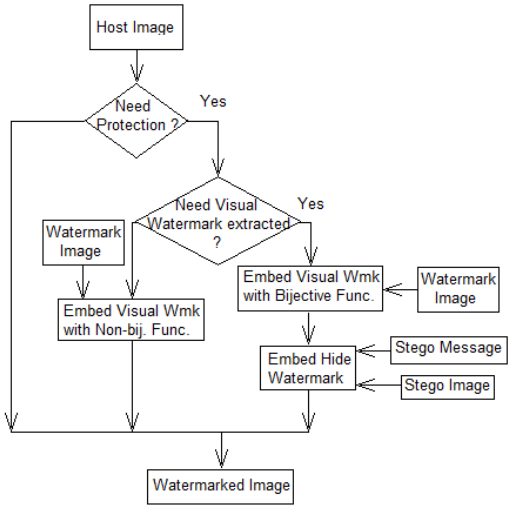


**Figure 4.Framework's owner module**.

On the receiver sideis checked if the hide watermark signature (*Sid*) is the same with the license signature. If the user is licensed, is extracted from *Mw* the inverse function constant parameter *d*.The inverse embedding function is applied, in order to compensate the visual watermark and to recover the original host image R,which is identical with the original image. When the signature or license is missing the inverse function is not applied and the output image is the watermarked image.

## CONCLUSIONS

We purpose a framework to protect in a complete manner the processed image that is media broadcasted.Thecopyright protection but alsoimage forgery is ensured on the owner side, when the original image is prepared for the media distribution. The presented method permit a high robustness because both hide and visual watermarking techniquesare together applied in order to detect the certified user and, finally, to eliminate the visual watermarking.

The quality of recovered image after watermark extraction and compensation has a very good qualityin HVS perception, practically the recovered image is the same as the original image (figure 5).

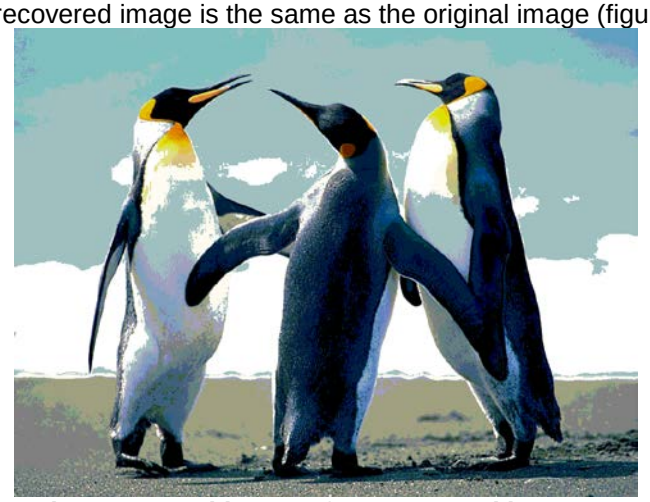

**Figure 5. The recovered image after watermarking compensation**

## BIBLIOGRAPHY:

[1] M Rogobete, L Răcuciu, "First and second order image statistics in specific image artifact detection", International Conference on Innovative Technologies, IN-TECH 2012

[2] M Rogobete, C Răcuciu, E. Rădoi "Original Methodology and Algorithm able to Identify Visible Noisy in Image and Video Stream", International Conference for Education and Creativity, 7th Edition, Bucharest, 2013

[3] M Rogobete, C Răcuciu, "Using Potential Field Analysis into Image Artifact Detection Field", Indian Journal of Research, May, 2014

[4] W Jiao, Y Fang, G He, "An Integrated Feature Based Method For Sub-Pixel Image Matching", The International Archives of the Photogrammetry, 2008 – Citeseer.

[5] Marius Rogobete, Ciprian Răcuciu - "Cryptographic Extension Key for Watermark Encoding" " Titu Maiorescu – 04.11.2014, International Conference for Education and Creativity

[6] Marius Rogobete, Ciprian Răcuciu - "Visual Watermark Embedded Functions" Titu Maiorescu – 04.11.2014, International Conference for Education and Creativity

[7] Marius Rogobete, Ciprian Răcuciu - "An Improved Cryptographic Method in Watermark Encoding" , Indian Journal of Research, Volume IV, Issue III, March 2015

[8] Peter Krogh," The DAM Book: Digital Asset Management for Photographers", O'Reilly Media Inc., 2009

[9] M Rogobete, C Racuciu, M Pirloaga, F Medeleanu,"USING HIDE WATERMARK IN VISUAL WATERMARK EXTRACTION. ADVANTAGES. ALGORITHM.", SEA-CONF2015 (in process)