Applied Physics Research; Vol. 5, No. 6; 2013
ISSN 1916-9639 E-ISSN 1916-9647
Published by Canadian Center of Science and Education

Biometric-Like Approach for Verifying Artworks Authenticity

Lorenzo Cozzella[1], Giuseppe Schirripa Spagnolo[1] & Fabio Leccese[2]

[1] Department of Mathematic and Physics of University "Roma Tre", Roma, Italy

[2] Department of Science of University "Roma Tre", Roma, Italy

Correspondence: Lorenzo Cozzella, Department of Matematic and Physics of University "Roma Tre", Via della Vasca Navale 84, Roma 00146, Italy. E-mail: lorenzo.cozzella@gmail.com

Received: October 18, 2013 Accepted: November 7, 2013 Online Published: November 25, 2013

doi:10.5539/apr.v5n6p118 URL: http://dx.doi.org/10.5539/apr.v5n6p118

Abstract

The artwork market is plenty of unauthorized reproduction of original products. One of the most varies filed is the counterfeiting of Authenticity Certificate related to paints, lithography, sculptures, etc., with the aim to create an illegal market of reproduced copies. To resolve this problematic, it is possible change the current paper certificate, related to a single artwork, with a digital version, which will contain some specific information, related to the artwork itself. In this paper, starting with the well-known advantages given by the biometry paradigm in human authentication, we propose a method able to distinguish the single "non-living" objects. In other words, we propose an approach that, by using the random inimitably characteristics, is able to uniquely identify artworks such as painting, lithographs, sculptures, etc. In this way it could be possible creating a secure digital certificate of authenticity (digital COA). Due to the high density information available in modern acquisition media, it is possible using a Speckle Metrology approach. During verification phase, the same area has to be acquired, to extract embedded verification data. It is possible to secure this data using a private key, necessary for accepting the digital signature. The presence of possible geometrical distortions between image present in the certificate and acquired during the verification phase, it is necessary applying geometrical corrections based on affine transformation, before executing the correlation methodologies, used in speckle metrology.

Keywords: artworks authentication, biometry, hylemetry, image processing, speckle metrology

1. Introduction

When we purchase a work of art, the main problem is to obtain a genuine certificate of authenticity (COA).

There is a great misuse of "certificate of authenticity"; if the COA is not directly originated by the artist, it is pretty much meaningless. In any case, even if the certificate of authenticity shall be made by the artist, in general, is relatively simple to clone it. Moreover, the certificate of authenticity is very often directly made by the seller.

In a simple, a dishonest seller can duplicate both the certificate of authenticity that the work of art. In this way, a copy of the certificate of authenticity can be used to pass off as a genuine a non-original work.

Figure 1 shows some examples of "classic" paper certificates of authenticity, and it is pretty clear to see they are relatively easy to fake.

Figure 1. Examples of "classic" Certificate of Authenticity (COA)

Generally, it is considered artworks with associate COA as "original", but this assertion is far to be the truth (Merriman, 1992). These occurs since does not exist rules to define who is (or is not) authorized to produce certificates of authenticity, or what information a COA must contain. For this reason, it is possible to anyone produce a certificate of authenticity, and insert into them also false or misleading information. On the other hand, dishonest merchants produce false COA. Generally, these fake certifications are used to "increase" the value of works (attribution of the work to an artist more important) or to deal in as original a copy (Nytimes, 1922).

A potential swindle can be carried out according to the schema below. A merchant buys a genuine work of art with its original COA. Then, he duplicates the work as well as the certification of originality and sells the work cloned. He, on this way, recovers (at a profit) the amount spent to buy the original and remains in possession of the genuine work. A famous forgery of artworks is created by Ely Sakhai; the owner of a Lower Manhattan Gallery, Exclusive Art. Mr. Sakhai acquired genuine, but lesser known works of Gauguin, like the lilacs, and other impressionist and modern artists, then ordered copies made by skilled forgers. Subsequently Mr. Sakhai sold the copies to private collectors, primarily in Japan and Taiwan. After years in the forgery trade, in an attempt to double his profits, Mr. Sakhai decided to sell some of the originals in his possession. He offered the Gauguin work, titled "Vase de Fleurs (Lilas)" to Sotheby's for the 2000 auction, at the same time as a copy he had sold to a customer in Tokyo was put up for auction at Christie's. But for that coincidence, the forgery might never been detected (Nytimes, 2004).

One solution to this problem would be put in action a procedure that couples, in an indissoluble way, the COA and the artwork to which it relates. In this way the use of a false certificate it is not more possible. To achieve this goal it is essential, for a particular work of art, to find distinctive, unrepeatable, and unchanged features. If these aspects exist, we have the ability to characterize the work of art and to discriminate it from another one. Many papers describe different approaches to identify, in inanimate objects, unique and non-reproducible features (Haist & Tiziani, 1998; Buchanan et al., 2005; Ingenia, 2011; Cowburn, 2008; Chong et al., 2008; Samuel et al., 2010).

In this paper we will implement a process like biometric identification, called hylemetry in precedent works (Schirripa Spagnolo et al., 2010a, 2010b, 2011; Cozzella et al., 2012a). In particular, similarity with biometry are reported, than a method based on speckle-like pattern is proposed, to be used on different artworks, such as (but not only) oil paints, lithography and sculptures. The term hylemetry derives from who Aristotele called the "non-living matter" (Huby, 1974).

This paper is organized as follows. In Section 2 the method used (hylemetric authentication) is described. In Section 3 we discuss the application of hylemetry identification of works of art; in other words, how to achieve a certificate of authenticity very difficult to fake or to clone. In Section 4 we deal with the problem of how you use the hylemetry to authenticate an artwork. The experimental results are given in Section 5. Finally, Section 6 contains the conclusions.

2. Biometry vs. Hylemetry

2.1 Introduction to Hylemetry

The traditional ways for establishing the authenticity of sensible objects, such as documents, banknotes, packaging and high value products rely on the presence of secret identifiers or on complex's manufacture process, which is hard to overcome, or counterfeit. Classic examples are barcodes, holograms, RFID, etc.

In any case has to be considered that the difficulty to duplicate, it does not mean inability to duplicate: "what one man can make, another can copy" (Nmab, 1993). Observe that conventional RFIDs could be easily copied and counterfeited and thus, are not capable of resolving the problem or tag authenticity (DeJean & Kirovski, 2006, 2010).

Currently, the unique identification of persons process is based on use of non-reproducible physiological or behavioral characteristics. Distinctive biometric features enclose fingerprints, hand geometry, retina, iris patterns, voice waves, DNA, handwrite signatures, etc.; this methodology is called biometric authentication (Woodward et al., 2002).

Biometric authentication is centered on the acquisition of individual human physical qualities, used to compose a template (feature vector) for further biometric identification (Woodward et al., 2002; Jain et al., 2011).

This template is compared with that extracted during the testing phase to determine whether a person is who he claims to be. Because of difficulty of acquiring in different phases, and with different acquisition systems, the same model, a verification method based on a set of thresholds is expected.

For an inanimate object, any model made to a particular technology can be replicate employing like tools. On the other hand, each pattern generated by random processes is a feature not replicable that can be exploited for hylemetric identification (Melen, 1999; Zhu et al., 2003).

2.2 Hylemetric Characteristics

In biometric authentication, the acquired feature should have the following properties (Cozzella et al., 2012b):

- Universality: characteristic has to be present in all the individuals;
- Permanence: characteristic stable over time;
- Uniqueness: samples related to different individuals should be as unlike as possible;
- Robustness: samples related to the same individual should be as close as possible;
- Availability: easy to acquire with a dedicated sensor;
- Acceptability: people shall consider the acquisition method as nonintrusive;
- Forge Resistance: the acquisition system should be arduous to deceive.

A system used for authentication of non-living objects (hylemetric authentication), should have similar properties.

In general, in hylemetric verification the feature vector (template) should have the following characteristics (Clarkson et al., 2009):

- Exclusivity: Each object must be distinguishable from all others;
- Stability: feature vector should be confirmable by multiple entities for all lifetime of the object;
- Shortness: template should be short and easily computable;
- Resistance to imitation: feature vector should be hard or impossible to duplicate; an object in such a way that the clone to express the same template as the original one.

Each random or hard-to-reproduce texture, can be potentially exploited in as hylemetric features. Good hylemetric features have to content also the following necessities:

- it has to be simple repeatable and reliable to extraction the feature vector;
- the template must be manufactured at low cost, compared with a chosen level of security;
- the cost of exact or near-exact replication of the random structure employed as hylemetric features has to be significantly greater than the commercial value of the cloned object;
- the cost of the authenticity verifying procedure has to be small, again compared with a chosen level of security.

3. Hylemetric Characteristics Identification on Artworks

In any artwork is possible finding a characteristic, which matches with the previous reported lists. In particular, artworks, due to the way on which they are produced, have an intrinsic randomness, due to the hand-made process. Analyzing some different examples, reported in Figure 1, it is possible identifying speckle-like structures in all of them. Figure 2(a) reports an oil paint, with highlighted the certificate area, Figure 2(b) shows the same information related to a lithography, and Figure 2(c) related to a sculpture. The process to create a hylemetric digital certificate of authenticity is based on the extraction, from a specific area of an artwork, of a random pattern difficult/impossible to reproduce. This allows defining the hylemetric approach as a one-way function (Goldreich, 2001), defined in the following as Hylemetric Hash Pattern (*HHP*). The *HHP*s extracted from the reported examples are shown in Figure 2 too. It is easy to notice that the three *HHP*s, even if extracted from three different artworks, and produced with different instruments and techniques, are very similar.

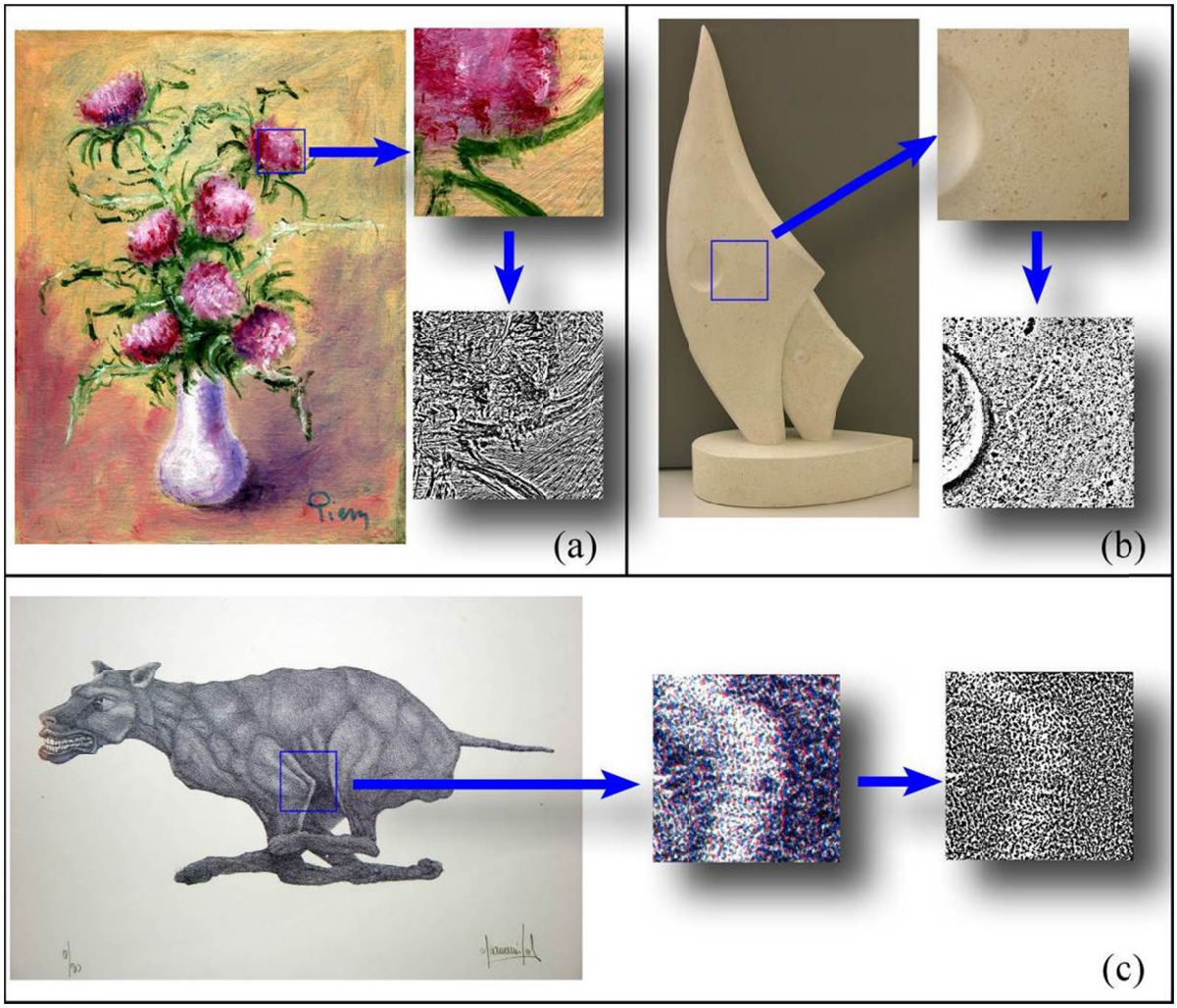

Figure 2. (a) oil paint; (b) stone lithography (c) sculpture

If we refer, for sake of simplicity, only to oil paint, reported in Figure 2(a), the first step is identifying an acquisition area and, inside it, selecting the trust points. The trust points are used to allow the correction of geometrical distortion that can be introduced in verification phase.

Figure 3(a) shows the oil painting and the related identified authentication area. On the authentication area (Figure 3(b)) are reported the trust points (four in this example). Figure 3(c) shows the area acquired during verification phase and the related trust points used to geometrically correct this image before the matching phase. The next step, is the construction of a *HHP* related to information acquired in the interested area. In the reported

example, the *HHP* is carrying out with a grey-leveling, high pass filtering, normalization, and subsequent thresholding (see Figure 3(d)). The result has speckle-like appearance, allowing to applying, in verification phase, typical speckle metrology techniques, as described in the following sections. The image shown in Figure 3(b) is inserted (with low resolution) in a digital authenticity certificate. On the digital authenticity certificate will be also present the *HHP* related to the authentication area. To avoid certificate digital counterfeiting, it has to be digitally signed, using a classic Digital Signature approach (Digital Signature Standard - DSS), based on PKI infrastructure (FIPS, 2013).

In other words, in the digital certificate of authenticity we have: the verification area in low definition ($I_C^{(LD)}$), the trust points, the Hylemetric Hash Pattern encrypted (HHP_C^*), the decryption key.

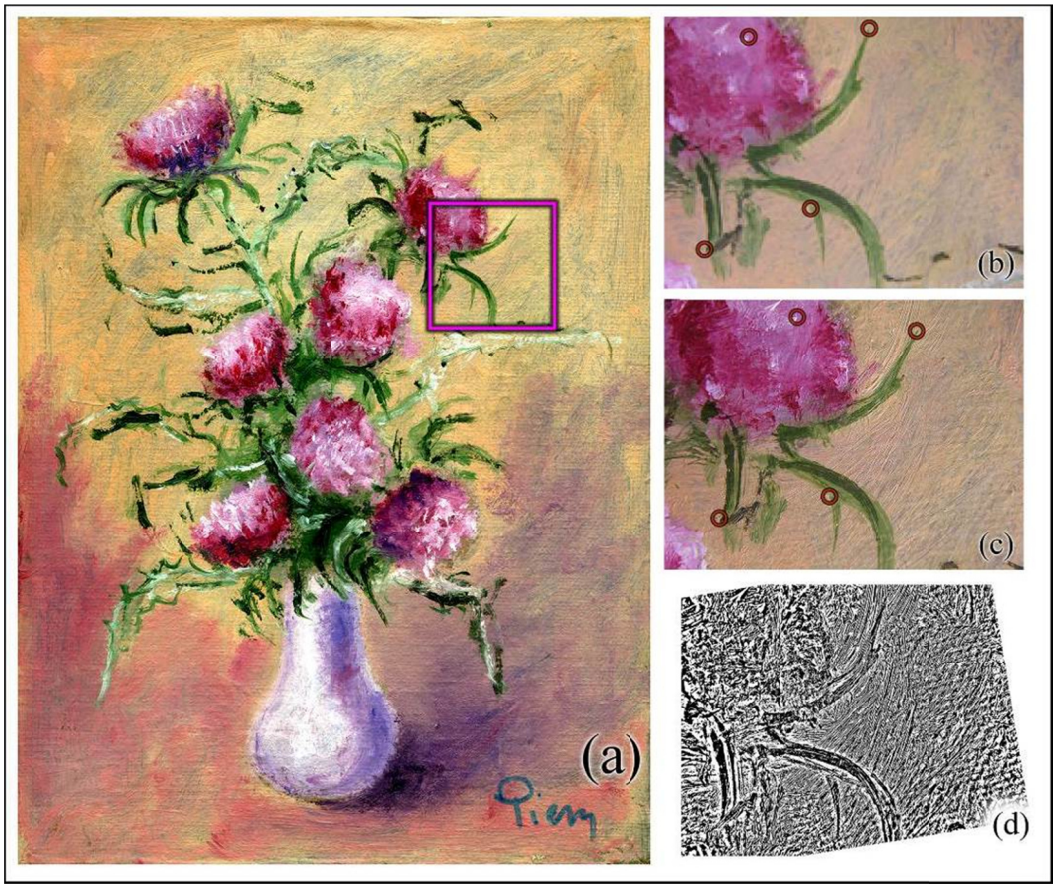

Figure 3. (a) oil painting with authentication area; (b) authentication area with trust points; (c) area acquired during verification phase; (d) Hylemetric Hash Pattern – *HHP*

4. Hylemetric Verification Phase

The first step to verify the authenticity of artworks (in our example oil paint) consists of acquiring the image of the authentication area (I_T − Test Image). During the process of acquisition it is not possible acquiring an identical zone to that present in the certificate of authenticity. Besides, some geometric distortions can be introduced. In other words, acquiring the authentication area with a typical digital camera, it is easy that we get a bigger or smaller piece of image around the interested region (with consequent scale error introduction), with some roto-translation (referred to original certification image). Also, the image can be full of distortions introduced by the optics system itself (e.g. barrel). To correct all the reported distortions, the system, by means of trust points, applies image transformations (e.g. polynomial, affine, reflective, etc.) so that Test Image (I_T) becomes very similar of the image (I_C) linked to Hylemetric Hash Pattern present in the digital certificate authentication. As described in (Gonzales, 2009; Vandome, 2010) is possible adjusting a great quantity of errors defining the correct amount of trust points on the two figures. Trust points are locations present in both the two

images, which identifying the same real point.

In this work, we have used affine transformations to achieve the correction of geometric distortions. Verification software, after having acquired the trust points, applies the correct transformation, which allows obtaining a corrected version of I_T to be used during matching phase.

After having applied geometrical transformation, it is possible extracting the HHP_T from the transformed image I'_T. The process is the same used for creating the HHP_C related to certificate image (the necessary procedure to obtain HHP_T must be reported on the digital certificate authentication).

The last step consisting in matching HHP_C and HHP_T, the Hylemetric Hash Pattern extracted from the digital authenticity certificate (and related to I_C), and from the geometrically corrected test image I'_T respectively.

Due to possible residual geometrical distortion and presence of noise, it is usual to obtain a *HHP* different in comparison to that present in the authenticity certificate, also in case of original artwork verification. Therefore, considering that the *HHP* has a casual structure, to allow the comparison among HHP_T and HHP_C, in this paper a verification approach based on digital cross-covariance calculation is proposed, similar to the one used in speckle field measurement (Sjödahl, 2000).

In this work, the used cross-covariance formula is:

$$C_\alpha(\Delta x, \Delta y) = F^{-1}\left[\frac{F^*(HHP_C)F(HHP_T)}{\left|F^*(HHP_C)F(HHP_T)\right|^\alpha}\right]. \quad (1)$$

In Equation (1) $(\Delta x, \Delta y)$ represent the correlation peak coordinates, where F and F^{-1} are forward and backward Fourier Transform operators, respectively, and * indicates the complex conjugate.
The Equation (1) can be efficiently calculated using a Fast Fourier Algorithm (Brigham, 1988). The coefficient α has the aim to control the correlation peak width. Optimum values range are from α = 0 for image characterized by high spatial frequency content and high noise level, to α = 0.5 for low noise image with less fine structure. For α values greater than 0.5 the high frequency noise is magnified. In our experiment we have always used α = 0.5 values.

As in biometric approach, also Hylemetry introduces a correlation threshold, necessary to define if the two *HHP* are similar enough to be considered the same. The threshold used in this paper is defined as follow:

$$\begin{cases} C_\alpha < T_\alpha & \text{false artwork} \\ C_\alpha \geq T_\alpha & \text{genuine artwork} \end{cases}. \quad (2)$$

The appropriate threshold is chosen in such a way as to minimize the False Acceptance Rate (Jain et al., 2011), such as the percentage of fake artworks identified as genuine, respect the total quantity of authentication checks. It has to be observed that the introduction of geometrical adjustment has highly reduced False Rejection Ratio, due to genuine artwork recognized as counterfeited.

Figure 4 shows the previously described process in a visual and schematic way.

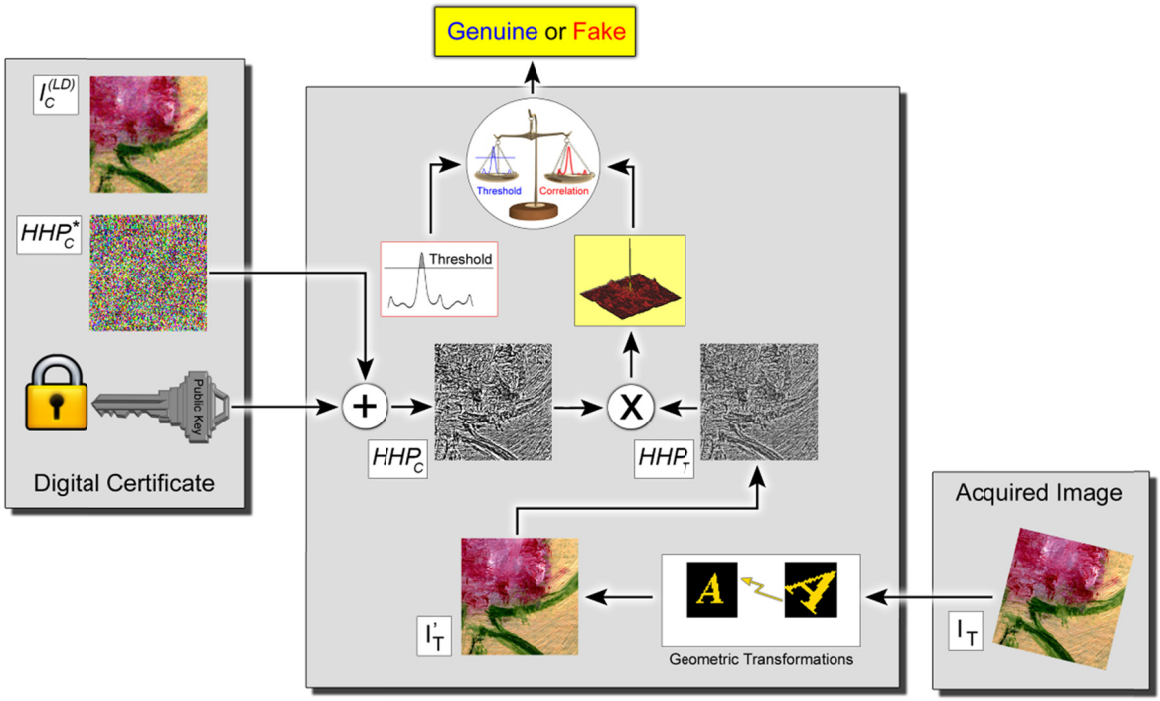

Figure 4. Complete schema showing the artwork verification phase

5. Experimental Results

Here we report some preliminary experimental tests performed on oil paints.

Initially, we have tested the robustness of the system to the acquisition of the test image with different illuminations and by different operators on the oil painting shown in Figure 3. For their execution we have design a specific software using the well-known simulation program Matlab©, which allows the human verifier to select verification areas among the two images, to input the trust points, having also a help system for selecting the same points on the two images. This software is also able to add controlled noise on the test image for testing noise strength, against different noise parameters. The developed software does not implement any automatic solution, which is a possible enhancement to the previously described procedure.

These first tests were performed using a commercial Nikon Coolpix 8700 Camera, with embedded Nikkor ED 8.9–71.2 mm objective, staying in front of the interested artwork area at ≈ 10 cm with macro function.

Figure 5 reports an example of extracted HHP_T. In Figure 5(a) we have the image of the authentication area ($I_C^{(LD)}$); this image is a low definition copy of the image I_C used to extract HHP_C. The image $I_C^{(LD)}$ is needed to identify the authentication area and the position of the trust points used for geometric correction. copy the texture from the original and "print" it in the copy (Kutter, 2000). The usage of a low definition copy, instead of the original one, on the printed version of the digital certificate, allows to avoid any possible copy attack, i.e. use of the reported area superposed on the counterfeited one to bypass the system. In Figure 5(b) we have Test Image; the image is acquired during the verification procedure. In Figure 5(c) the HHP_C and in Figure 5(d) the HHP_T are finally reported. Moreover, we report 2D correlation between HHP_C and HHP_T before (Figure 5(e)) and after (Figure 5(f)) geometrical correction.

In Figure 5, the correlation has been calculated using Equation (1). Figure 5(e) underlines how critical the geometrical distortions are for the proposed system. In particular, respect with a statistical Threshold equal to $T_\alpha = 0.31$, the normalized correlation peak is equal to $C_\alpha = 0.095$. On the contrary, with geometrical correction, we have a normalized correlation peak equal to $C_\alpha = 0.75$, where the threshold is equal to $T_\alpha = 0.34$, very similar to the previous one.

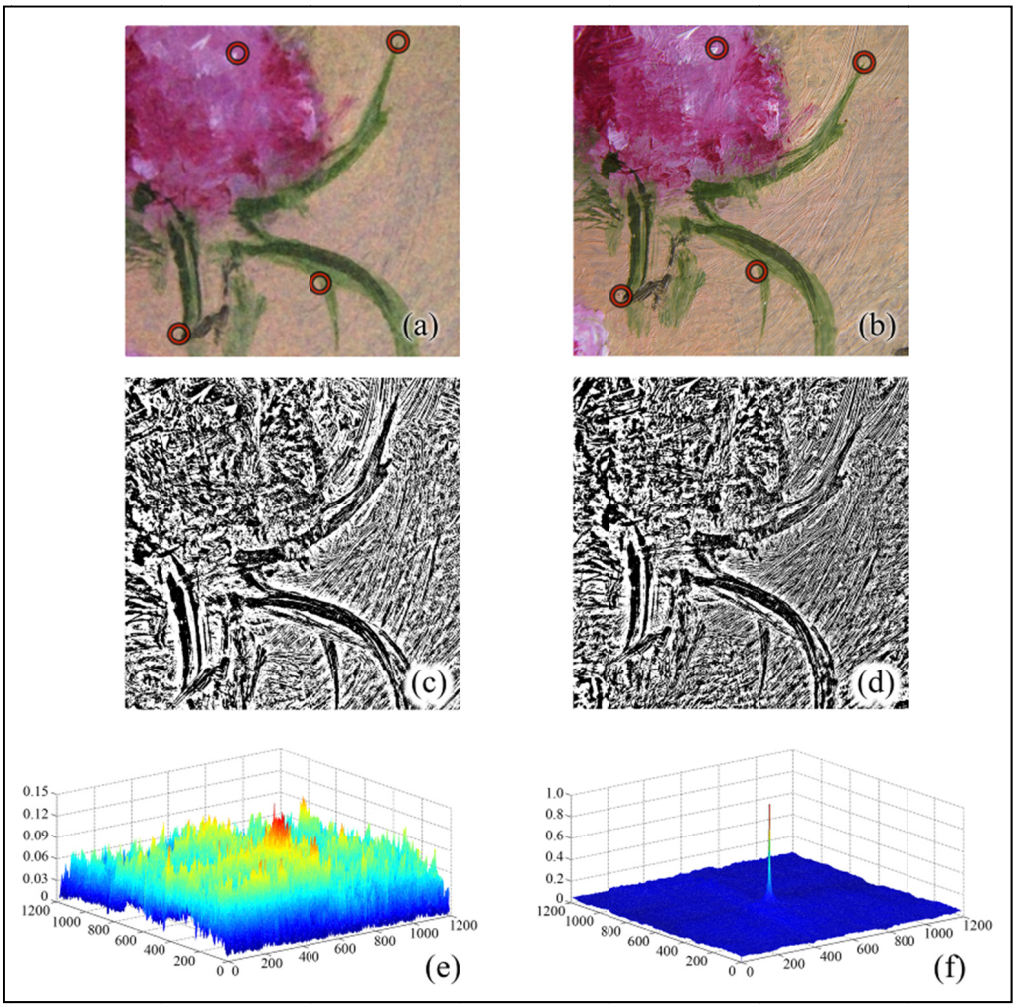

Figure 5. Example of extracted HHP_T. (a) $I_C^{(LD)}$ image; (b) I_T image; (c) HHP_C; (d) HHP_T; (e) 2D correlation between HHP_C and HHP_T without geometrical correction; (f) 2D correlation between HHP_C and HHP_T with geometrical correction

In Figure 6 is reported a similar example, where the test image, reported in Figure 6(b) has been acquired with 20% downscaling in both dimensions (i.e. acquisition from a distance greater than the original one), a 7 degree clockwise rotation, a horizontal translation of 111 pixel and a vertical one of 36 pixel, and a reduced acquired area. This extreme case allows testing the robustness of the system, which reports a 2D Normalized Correlation that still highlights a correct identification ($C_\alpha = 0.72$ versus $T_\alpha = 0.36$).

The threshold T_α used in this paper, for any reported results, is:

$$T_\alpha = 3 \cdot \sqrt{m_C + \sigma_C} \ . \tag{3}$$

where m_C is the mean value of the correlation function and σ_C the related standard deviation. It has to be noted that is always possible to define alternative statistical thresholds. We have used in our experiments also different thresholds, with similar results, such as three times the mean value plus once standard deviation, three times the standard deviation plus once mean value and so on. The choice of the threshold in Equation (3) is due to the very low variance of its values among different image distortions.

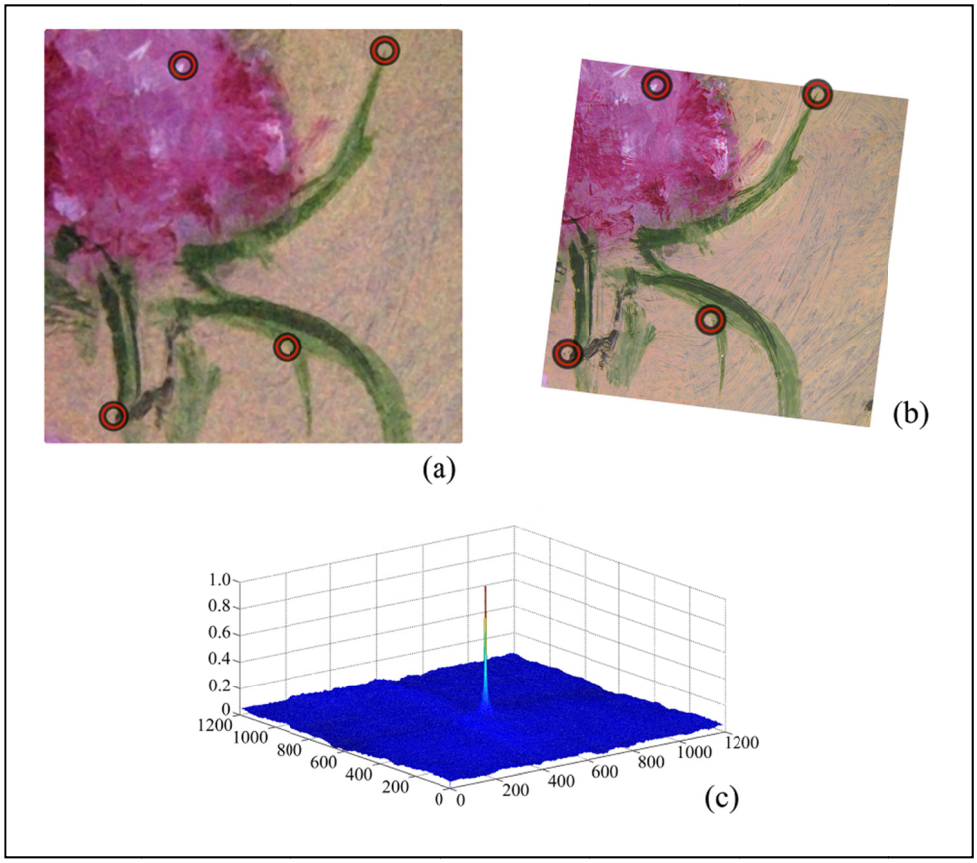

Figure 6. Example of 2D correlation obtained with test image having "important" geometric distortions. It is possible to observe that the geometric corrections allow, also in this case, to correctly calculating the cross-covariance

All tests conducted to demonstrate the correct extractability of HHP_T have shown that it is possible to extract the required Hylemetric Hash Pattern. We also found that the choice of a threshold obtained with the Equation (3) (in generally we have $0.25 < T_\alpha < 0.4$) allows an efficient recognition; the correlation coefficient was always significantly higher than the threshold ($0.5 < C_\alpha < 0.9$)

Subsequently, to test our method on commercial copies, we bought two copies of the Van Gogh painting: Tournesols (sunflowers); both copies made by the same artist (see Figure 7).

Figure 7. Two copies of the Van Gogh painting "sunflowers"

The two paintings shown in Figure 7 are similar. Unfortunately, since they are made "by hand" with the artist not informed of the purpose for which they were expected, they show significant differences. Therefore, to test our method we chose as authentication area, the zone with greater similarity between the two paintings.

The experiments were conducted to verify the possibility to discern the two different copies. The Figure 8(a) shows the acquisition area and the trust points; the acquisition zone has been chosen considering the area where the texture presents greater variability. The Figure 8(b) shows the correspondent HHP_T.

Figure 8. (a) authentication area with trust points; (b) Hylemetric Hash Pattern – *HHP*

For the two paintings we have acquired the reference zone with three different cameras: Nikon Coolpix 8700; Iphone 5 with external 15X macro system (Carson LensMag 15X); Samsung ES20. Figure 9 shows the six acquired images. It as to be noted that any single acquisition has been carried out under different lighting conditions.

Figure 9. Acquired image of both paintings through three different cameras

For each of these six images we have extracted the *HHP*s and then, through the Equation (1) we have calculated the corresponding correlation coefficients. Table 1 shows obtained correlation coefficients. From this table, it is easy to see that the system is able to distinguish the two different copies, even when the reference images are acquired with different devices.

Table 1. Correlation coefficients obtained from the HHPT linking to six images present in Figure 8.

	Sunflowers (a) Nikon	Sunflowers (a) Iphone 5	Sunflowers (a) Canon	Sunflowers (b) Nikon	Sunflowers (b) Iphone 5	Sunflowers (a) Canon
Sunflowers (a) Nikon	**1**	0.73	0.81	0.13	0.09	0.15
Sunflowers (a) iphone 5	0.65	**1**	0.67	0.22	0.18	0.23
Sunflowers (a) Samsung	0.72	0.66	**1**	0.19	0.20	0.18
Sunflowers (b) Nikon	0.25	0.21	0.77	**1**	0.80	0.68
Sunflowers (b) iphone 5	0.12	0.24	0.69	0.78	**1**	0.74
Sunflowers (b) Samsung	0.22	0.11	0.70	0.74	0.67	**1**

The tests do not cover all possible cases and all kinds of works of art. In any case, these preliminary tests well prefigure the possibility to use this methodology for safely certifying the authenticity of a work of art with an high level of reliably.

6. Conclusion

In this paper an innovative methodology, founded on Hylemetry, was demonstrated, which allows to produce not duplicable certificate of originality. The chosen hylemetric characteristic allows to obtain high verification rates, thanks also to a geometrical correction preprocessing, executed in manual way, to correct errors and misalignments of acquisition during the verification procedure. The proposal method allows to generate a unique, Hylemetric Hash Pattern, used for verifying object authenticity. The usage of a well-known and highly consolidated speckle metrology matching algorithm allows to be confident on the obtained results and the robustness of the procedure. It is also possible to implement a securing method, based on DSS, for protecting digital certification of authenticity from copy attack, the most used method in this situation. Future studies for obtaining an automatic system able also to determine an optimum threshold, are in progress, with the aim to be independent from the interested object.

Very recently, the van Gogh museum and the FUJIFILM Belgium have developed a new and unique reproduction process able to reproduce the textured detail of Van Gogh's artworks in accurate color. This new method of reproduction of the paintings allows you to achieve the best fine art replicas ever seen. These copies replicate exactly the format, the color brightness, and texture of the original (Fujifilm, 2013; Van Gogh Museum, 2013). In future studies we want to verify whether our method works well on these copies of the highest quality. In particular we will try to check if you can distinguish a copy from the original and a copy from another.

References

Brigham, E. O. (1988). *The Fast Fourier Transform and its applications*. New Jersey: Prentice-Hall, Upper Saddle River.

Buchanan, J. D. R., Cowburn, R. P., Jausovec, A. V., Petit, D., Seem, P., Xiong, G., … Bryan, M. T. (2005). Fingerprinting' documents and packaging. *Nature, 436*, 475. http://dx.doi.org/10.1038/436475a

Chong, C. N., Jiang, D., Zhang, J., & Guo, L. (2008). Anti-counterfeiting with a Random Pattern. *Proceedings of SECURWARE 2008*, 146-153. http://dx.doi.org/10.1109/SECURWARE.2008.12

Clarkson, W., Weyrich, T., Finkelstein, A., Heninger, N., Halderman, J. A., & Felten, E. W. (2009). Fingerprinting Blank Paper Using Commodity Scanners, *SP'09—Proceedings of 30th IEEE Symposium on Security and Privacy*, 301-314. http://dx.doi.org/10.1109/SP.2009.7

Cowburn, R. P. (2008). Laser surface authentication—reading Nature's own security code. *Contemporary Physics*, *49*(5), 331-342. http://dx.doi.org/10.1080/00107510802583948

Cozzella, L., Schirripa Spagnolo, G., & Simonetti, C. (2012a). Drug packaging security by means of white-light speckle. *Optics and Lasers in Engineering, 50*(10), 1359-1371. http://dx.doi.org/10.1016/j.optlaseng.2012.05.016

Cozzella, L., Simonetti, C., & Schirripa Spagnolo, G. (2012b). Is it possible to use biometric techniques as authentication solution for objects? Biometry vs. hylemetry, *5th International Symposium on Communications Control and Signal Processing (ISCCSP)*. 1-6. http://dx.doi.org/10.1109/ISCCSP.2012.6217753

DeJean, G., & Kirovski, D. (2006). Making RFIDs Unique. *Radio Frequency Certificates of Authenticity, IEEE Antennas and Propagation Society International Symposium*. July 2006, pp. 1-6. http://dx.doi.org/10.1109/ISCCSP.2012.6217753

DeJean, G., & Kirovski, D. (2010). Can A Physically Secure RFID Be Produced? A Review of RFDNA. *Proceedings of the Fourth European Conference on Antennas and Propagation, CCIB*, Barcelona, Spain 12-16 April 2010. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05504992

FIPS (Federal Information Processing Standards) PUB 186-4. (2013). *Digital Signature Standard (DSS).* Retrieved from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Fujifilm (2013). *Premium three-dimensional replicas of Van Gogh masterpieces*. Retrieved from http://www.fujifilm.eu/eu/news/article/news/premium-three-dimensional-replicas-of-van-gogh-masterpieces

Goldreich, O. (2001). *The Foundations of Cryptography - Volume 1.* Cambridge University Press.

Gonzales, R. C., Woods, R. E., & Eddins, S. L. (2009). *Digital Image Processing using Matlab* (2nd ed.). Gatesmark Publishing.

Haist, T., & Tiziani, H. J. (1998). Optical detection of random features for high security applications. *Opt. Comm., 147*(1-3), 173-179. http://dx.doi.org/10.1016/S0030-4018(97)00546-4

Huby, P. M. (1974). Review of Heinz Happ 'Hyle: Studien zum aristotelischen Materie-Begriff. *The Classical Review (New Series), 24*(1), 44-46. http://dx.doi.org/10.1017/S0009840X00241711

Ingenia (2011). Identity, Secure Documents & Anti-Counterfeiting. Retrieved from http://www.ingeniatechnology.com/wp-content/uploads/2011/04/ING_SDWReport.pdf

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Berlin: Springer.

Kutter, M. K., Voloshynovskiy, S., & Herrigel, A. (2000). *The Watermark Copy Attack*, in Proc. SPIE, *Security and Watermarking of Multimedia Contents II*, Vol. 3971, pp. 371-379. San Jose, CA. http://dx.doi.org/10.1117/12.384991

Melen, R. (1999). Record document authentication by microscopic grain structure and method, *European Patent Specification* EP0570162B 1999/05. http://www.google.com/patents/EP0570162B1?hl=en

Merriman, J. H. (1992). Counterfeit Art. *International Journal of Cultural Property, 1*(1), 27-28. http://dx.doi.org/10.1017/S0940739192000055

Nmab. (1993). Counterfeit Deterrent Features for the Next-Generation Currency Design, *Publication Nmab, 472 - National Academies Press Washington, D.C*. http://www.nap.edu/openbook.php?record_id=2267

Nytimes (1922). New York Times, *Art Counterfeit Revealed*, 1922, September 24. http://query.nytimes.com/mem/archive-free/pdf?res=F60A14F63A5D1A7A93C6AB1782D85F468285F9

Nytimes (2004). New York Times, *Art Gallery Owner Pleads Guilty In Forgery Found by Coincidence*, 2004, December 14. http://www.nytimes.com/2004/12/14/nyregion/14art.html

Samuel, W., Uranus, H. P., & Birowosuto, M. D. (2010). Recognizing Document's Originality by Laser Surface Authentication, *Proceeding of Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*, 37-40. http://dx.doi.org/10.1109/ACT.2010.15

Schirripa Spagnolo, G., Cozzella, L., & Simonetti, C. (2010a). Banknote security using a biometric-like technique: a hylemetric approach. *Meas. Sci. Technol., 21*(5), 055501. http://dx.doi.org/10.1088/0957-0233/21/5/055501

Schirripa Spagnolo, G., Cozzella, L., & Simonetti, C. (2010b). Currency verification by a 2D infrared barcode. *Meas. Sci. Technol., 21*(10), 107002. http://dx.doi.org/10.1088/0957-0233/21/10/107002

Schirripa Spagnolo, G., Cozzella, L., & Simonetti, C. (2011). Hylemetry versus Biometry: a new method to certificate the lithography authenticity, *Proc. SPIE 8084, O3A: Optics for Arts, Architecture, and Archaeology III*, 80840S. http://dx.doi.org/10.1117/12.889387

Sjödahl, M. (2000). Digital speckle photography, *Trends in Optical Non-destructive Testing and Inspection* (pp. 179-185). Amsterdam: Elsevier Publishing.

Vandome, F. P., Mcbrewster, A. F., & Miller, J. (2010). *Affine Transformation* (Beau-Bassin, Mauritius, Alphascript Publishing).

Van Gogh Museum. (2013). *Van Gogh Museum launches Relievo collection of Van Gogh masterpieces in Hong Kong*. Retrieved from http://www.vangoghmuseum.nl/vgm/index.jsp?page=327966&lang=en

Woodward Jr., J. D., Orlans, N. M., & Higgins, P. T. (2002). *Biometrics*. Berkeley, CA: McGraw-Hill/Osdorne.

Zhu, B., Wu, J., & Kankanhalli, M. S. (2003). Print signatures for document authentication, in *Proc. 10th ACM Conf. on Computer and Communications Security*, 145-154. http://dx.doi.org/10.1145/948109.948131