ACTA IMEKO
ISSN: 2221-870X
September 2015, Volume 4, Number 3, 65 - 71

Painting authentication by means of a biometric-like approach

Giuseppe Schirripa Spagnolo[1], Lorenzo Cozzella[1], Maurizio Caciotta[2], Roberto Colasanti[3], Gianluca Ferrari[3]

[1] Università Roma Tre – Dipartimento di Matematica e Fisica, Via della Vasca Navale, 84, 00146 Roma, Italy
[2] Università Roma Tre – Dipartimento di Scienze, Via della Vasca Navale, 84, 00146 Roma, Italy
[3] Expert in protecting cultural heritage, Roma, Italy

ABSTRACT
Artwork counterfeiting is a wide problem in the art market, both for private subjects and museums. For this reason, it is important to introduce innovative authentication solutions, based on state-of-the-art technologies. In particular, in this paper, the proposed solution is based on a mobile architecture, starting from the consideration that nowadays mobile phones include quality photo and video cameras, access to wireless networks and the internet, GPS assistance and other innovative systems. The proposed solution uses smartphones as simple, robust and efficient sensor for artworks authentication. When we buy an artwork object, the seller issues a certificate of authenticity, which contains specific details about the artwork itself. Unscrupulous sellers can duplicate the classic certificates of authenticity, and then use them to "authenticate" non-genuine works of art. In this way, the buyer will have a copy of an original certificate to attest that the "not original artwork" is an original one. A solution for this problem would be to insert a system that links together the certificate and the related specific artwork. To do this it is necessary, for a single artwork, to find unique, unrepeatable, and unchangeable characteristics. In this article we propose an innovative and non-invasive method for the authentication of artworks based on random intrinsic object characteristics. This approach is based on biometry paradigm (analogue fingerprinting). The paper presents a stand-alone solution, and an internet-based one, necessary for granting security verification also in case of problems with the used RFID tag. The proposed method uses an RFID Tag and a 2D barcode, in conjunction with an Internet-based Authentication Archive.

Section: RESEARCH PAPER

Keywords: Painting authentication; RFID application; Random Features; smartphone application; Biometric-Like Approach

Citation: G. Schirripa Spagnolo, L. Cozzella, M. Caciotta, R. Colasanti, G. Ferrari, Painting authentication by means of a biometric-like approach, Acta IMEKO, vol. 4, no. 3, article 11, September 2015, identifier: IMEKO-ACTA-04 (2015)-03-11

Editor: Paolo Carbone, University of Perugia, Italy

Received February 17, 2015; **In final form** April 23, 2015; **Published** September 2015

Funding: This work was supported by MIUR

Corresponding author: G. Schirripa Spagnolo, e-mail: giuseppe.schirripaspagnolo@uniroma3.it

1. INTRODUCTION

The Artwork market is very complex and variegated, in which a single piece can have an incredible high value. In general, the value of an artwork is not always related to its intrinsic quality or characteristics, but on the possibility to demonstrate it was made by a famous artist. Therefore, the amount of money that can be paid for paint or artwork is strictly related to the expertise made by a well-known and authorized art expert. The output of an expertise is always a Certificate of Authenticity (CoA). Unfortunately, often these certificates are exchanged among similar artworks: the seller, to certificate the originality of more than one single artwork, supplies the same document. In this way, the buyer could have a copy of an original certificate to attest that the "not original artwork" is an original one. Unluckily, most people believe that art with a certificate is automatically genuine, but that is not even close to truth [1].

A possible fraud can be put the following way into effect. An art merchant, starting from an original artwork with original certificate of authenticity, can duplicate both and sell false artwork as genuine using false certificate of authenticity as clue of originality.

Museum objects are generally identified using some sort of cataloguing system. The objects may be (digitally) photographed, and then marked using a sticker, perhaps with a barcode, or a marker. This information can be considered as a fingerprint of the artwork and they may be entered into a paper or modern software catalogue/database along with other descriptive and historic information, condition reports, etc.

To authenticate an artwork, starting from the marker affixed on it, it is necessary to consult the Museum archive.

For private collections or works produced by living artist, we ust use a slightly different approach. The artist, or artwork expert, may photograph the artwork, describe it, and take photos at high resolution of the surface texture, yield a picture of him near the item and so on. In other words, an identity document is created and a unique set of fingerprints has to be identified [2], [3]. This file is archived, with the information and the author digital signature, in an opportune Artwork Digital Archive (ADA). The ADA software generates a unique artwork identification number and a dedicated URL (Universal Resource Locator), where this information is deployed. This process is similar to the digital object identifier (DOI) schema [4]. A DOI is a character string (a "digital identifier") used for uniquely identifying an object such as an electronic document. Metadata about the object is stored in association with the DOI name and these metadata may include a location, such as a URL, where the object can be found.

In this case, the ADA sends back to the author (or to the certification authority) the artwork URL and the author can put it on the lithography itself (for example on its back) by means of a 2D barcode or RFID tag attached to the artworks. By using an RFID tag with a high memory capacity, all (or part of) the information contained in the identity document can be duplicated in the chip bonded on the artwork.

A way to simplify the described solution would be the use of the technology offered by modern smartphones to connect to a proper website which would thus allow checking the origin of the artwork. The website, in this case, will be the ADA Database, designed to contain information about the artwork and a digital certificate of authenticity. This digital certificate links information on non-cloneable features of the specific artworks. In this way the inappropriate usage will not be possible and the buyer will be able to verify the originality by himself [5].

To do this it is necessary, for a single artwork, to find unique, unrepeatable, and unchangeable characteristics. If these characteristics are present, we have the possibility to identify the artwork and to distinguish it from another one [6]-[9]. By choosing the appropriate characteristic, such kind of identification can be applied to many types of artwork objects.

The rest of this paper is structured as follows: Section 2 outlines RFID tags and remote database authentication schema. Section 3 defines the artworks fingerprints and hylemetric template. Section 4 defines the safeart system and obtained result. Finally, Section 5 concludes the paper.

2. RFID SYSTEM

Radio Frequency IDentification (RFID) is a technology that allows a small radio device attached to an item to carry an identity for that item [10]. The first known use of RFID-like technology dates back to World War II time (1939), when British Royal Air Force used it for friend or foe aviation identification [11].

Radio frequency identification has attracted considerable press attention in recent years, and for good reasons: RFID not only replaces traditional barcode technology, it also provides additional features and removes boundaries that limited the use of previous alternatives. Printed bar codes are typically read by an optical system that requires a direct line-of-sight to detect and extract information. With RFID, however, a scanner can read the encoded information even when the tag is concealed for either aesthetic or security reasons—for example, embedded in an artwork (example: sandwiched between painting layers).

RFID is a wireless/contactless technology, avoiding remote manipulations, requires special protection service and risk management. A typical RFID system includes at least a tag (transponder), a reader (interrogator with antenna) and a data processing environment, which operates the obtained data. The RFID-enabled mobile phones may function as processing unit. In this case, the reader and the processing unit are integrated to one handheld device (Figure 1) [12]. Due to many possible uses of RFID, there are a lot of differences in its system components: different types of tags as well as a variety of readers.

The function of RFID systems may be described in the following way. Reader's antenna emits radio waves and once a tag (passive) is within the working range, it receives the radio signal. Then the tag responds back with its own data message. The reader decodes the received data from the tag and these data are passed to further processing.

Even the most important and characteristic feature of RFID systems—their unique identifier—is susceptible to attacks. Although in theory you cannot ask an RFID manufacturer to create a clone of an RFID tag [13], in practice replicating RFID tags does not require a lot of money or expertise considering the wide availability of writable and reprogrammable tags. An ominous example is the demonstration, by a German researcher, of the vulnerability of German passports [14].

In this paper, the problem of possible cloning of the RFID is not important. Authentication is done with the information contained into an RFID and robustness against forgery is granted to the fact that such information is related to specific characteristics of an individual work. As well as the fingerprints contained in an identity document, also Hylemetry approach avoids clone problems; fingerprints on the document are compared with those of the individual. Similarly, the fingerprints of the work (high resolution photo, surface texture, etc.) contained in the document of identity (RFID) are compared with those extracted from the work. In order to make an authentication system robust, a 2D barcode is linked to the RFID. In the 2D barcode is memorized the URL where a copy of the authentication information is stored.

To avoid copy attack, duplication/replacement of the fingerprint file, the use of a digital signature is also necessary [15]. A digital signature grants that a document is original. In

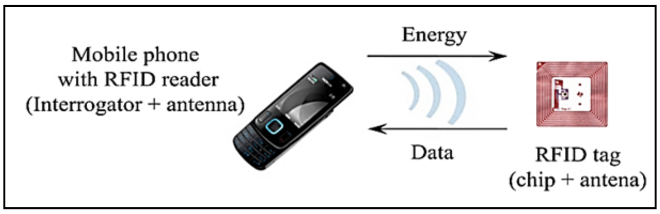

Figure 1. The mobile device as part of the RFID system.

this paper the template constructed from the artwork high-resolution image is original (i.e. constructed by the artwork author or by the certifier company). It links the identity of the underwriter with the file and provides an official stamp (unalterable otherwise the digital signature verification fails), which legally determines the author of the document. These characteristics can be efficiently exploited to combat the counterfeiting. The template (i.e. the fingerprint file) is digitally signed by an asymmetric key algorithm, an encrypting "two keys system", which exploits devices able to producing two different, but linked keys, one private (internal to the device and irretrievable) and the other public.

With the digital signature, we obtain an encrypted and signed copy of the fingerprint file itself; in this way, the data present in the certification media cannot be used for copy attack. Obviously, for verifying the artwork originality, it is necessary, using the associated public key k_{pub}, to decrypt the encoded information. The whole verification procedure can be implemented in an opportune application (app) that exploits the elaboration potentiality of smartphones.

Figure 2 shows the schema of the artwork's authentication step.

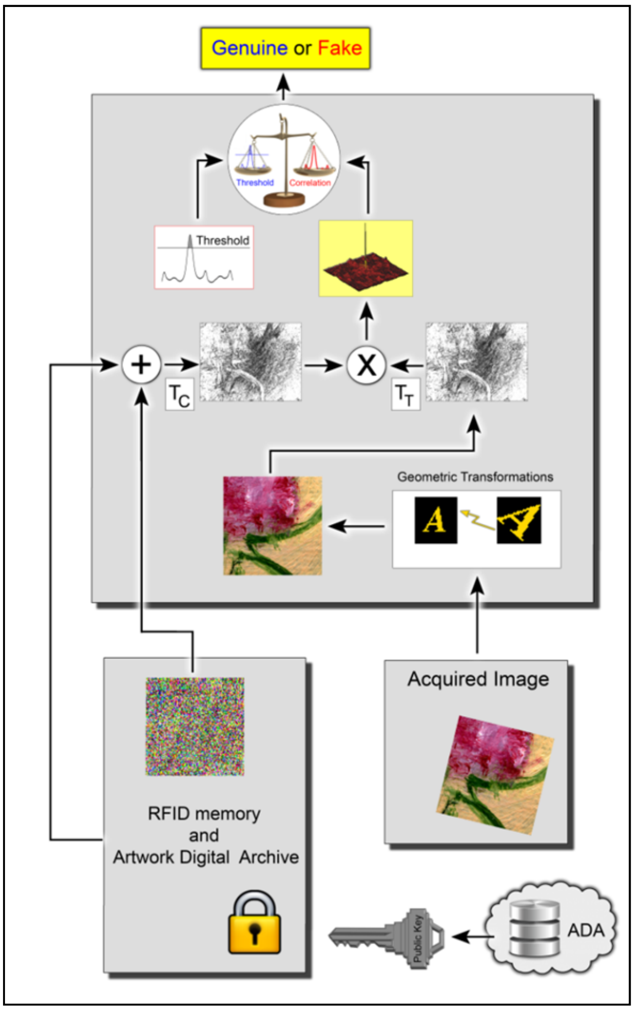

Figure 2. Schema showing the authentication step. In the figure not all information stored in the RFID is reported for easy understanding. T_T is the template extracted and geometrically corrected during authentication phase, T_C is the original template present in the CoA and T_C^* is the encrypted version of T_C.

As shown in Figure 2 the verification phase is based on the extraction of the fingerprint file directly from a precise portion of the artwork image. This leads to possible geometrical distortions. For this reason, the verification app on the smartphone, will be based on the Fourier - Miller Transformation, which automatically solves rotations, translations and scales, which are the most common errors introduced during the acquisition phases. We have used this kind of registration because our subjects are flat objects and, for avoiding any other image distortion (e.g., barrel), we have taken only the central part of the image itself (i.e., 1200 × 1200 pixels, starting from an acquired image of 3264 × 2448 pixels, typical dimensions obtained using an IPhone 5 or 5S and an appropriate external objective kit). Obviously in case of 3D objects to be authenticated, a more sophisticated Image Registration will be necessary, to still allow an automatic procedure.

At this point a possible stand-alone solution is based on using only a new generation smartphone and the information contained in the RFID. New generation smartphones are able to read information contained in passive RFID tags, using the NFC technology (if RFID tag data are conform to ISO 15693) or external wireless (i.e. Bluetooth) RFID reader. The smartphone can acquire from the RFID the information related to the verification area to be acquired, in low resolution, and the template, digitally signed, to be used in the verification phase. A dedicated application running on the smartphone can now acquire the requested area at high resolution, applying image registration and locally calculating the template on the basis of patterns obtained from the high resolution image (T_T). Eventually, a threshold-based correlation can be applied to verify if the two templates are as equal as necessary to be considered as related to the same artwork.

The presence of a template digitally signed in the RFID (T_C^*), requests for the verification application to know the public key of that template, for extracting the "readable" version to be compared with the locally calculated one (T_C). This step grants the protection against the copy attack, where an RFID tag is bounded onto a false artwork, containing false information: to do this the counterfeiter has also to have the private key used by the author for digitally signing all her/his work.

In any case, also for stand-alone solutions, the presence of the 2D barcode containing the ADA URL with all the necessary verification information is necessary. This because RFID lifetime, also in case of a passive one, cannot be compared with the artwork one, but the system has to grant a correct verification also in case of RFID reading failure. In this last case the verification is made using the data retrieved by the secure URL, given by the ADA. The ADA connection can be also available directly from the verification app. In fact, the RFID can contain also a unique identification code, such as the DOI used for bibliographical purposes [16], that allows the smartphone app to access the remotely maintained information on the ADA database for the investigated artwork, and obtain not only the data necessary to verify the artwork originality, but also artwork's and author's information as well as museum interesting data and so on. In this way the app suits both for verifying artwork authenticity and for acquiring artworks and authors information.

3. FINGERPRINTING

In human authentication, the sampled characteristic should have the following properties:

- Universal: every person should have the characteristic;
- Permanent: the characteristic should not vary over time;
- Distinctive: samples corresponding to different persons should be as different as possible, that is, the interclass variability should be as large as possible;
- Robust: samples corresponding to the same person should be as close as possible, that is, the intraclass variability should be as small as possible;
- Accessible: the sample should be easy to be presented to the sensor;
- Acceptable: it should be perceived as nonintrusive by the user;
- Hard to circumvent: it should be hard for an impostor to fool the system.

The fingerprints of an individual fully respond to these properties. As no two people in fingerprinting history have been found to have the same fingerprint, it can be said that a fingerprint may be used to uniquely identify a person.

Similar properties are required in the technique used for authenticating the inanimate objects. In particular, in the artworks authentication the sampled characteristic should have the following properties [17]:

- uniqueness: every object should be identifiable and distinguishable from all others;
- consistency: the feature vector should be verifiable by multiple parties over the lifetime of the object;
- conciseness: the feature vector should be short and easily computable;
- robustness: it should be possible to verify the feature vector even if the object has been subjected to harsh treatment;
- resistance to forgery: it should be very difficult and costly or impossible for an adversary to forge a document by coercing a second object to express the same feature vector as the original.

Each texture, that is highly random and difficult/impossible to reproduce, can be potentially used as hylemetric characteristic. Obviously, good characteristics for authenticate inanimate objects have to satisfy the following requirements:

- it has to be simple repeatable and reliable to implement the feature vector (template);
- the cost of creating and signing the feature vector has to be small, relative to a desired level of security;
- the cost to create an artwork clone able to generate the same template of the original one, has to be greater than the value of the object under forgery;
- the cost of verifying the authenticity of a signed feature vector has to be small, again relative to a desired level of security.

The method to authenticate an inanimate object is called Hylemetry, from the Greek "hyle" that means "non-living matter", and "metros", which means measurement. In this paper, the proposed authentication system is based on the identification and correct acquisition of a hylemetric characteristic and the related creation of a hylemetric template to be used inside the "RFID-based" safeart system. If we consider the certification of lithography we have considered as hylemetric unique characteristics the colorful "stains", acquired by means of a common high-level smartphone. Therefore, with the potentiality offered by modern smartphones referring to the processor power and image elaboration, these can be easily transformed into excellent biometric (hylemetric) sensors [18]. The smartphone used in this paper is a common iPhone 5 equipped with external objective Olloclip® 10× macro lens. Figure 3 shows the smartphone system during the acquisition, with the Olloclip external lens system added on it. This external lens system is necessary due to the actual limitation of the IPhone camera for macro acquisition. Using different kinds of smartphones (*e.g.* Nokia Lumnia 1200 or higer) this external lens kit is no more necessary.

Subsequently, the colorful "stains", acquired in RGB 24 bit format, are transformed to a uniform CIELAB color space [19]. After that, we use only the L channel, normalized with dynamic 0 to 1. In this way, we are sure that the obtained image is not affected by the environmental illumination. The obtained image has a typical speckle-like structure. This procedure is a one-way function. The Hylemetric Patterns, extracted from two Job's Dog Lithography (the 18th and 19th on a total number of 20 copies made by the author), used as examples are shown in Figure 4.

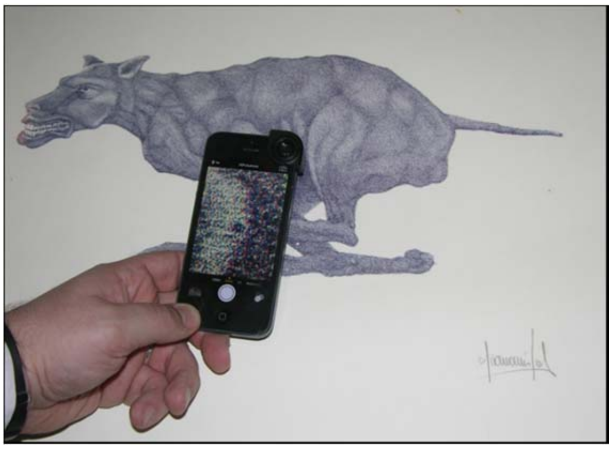

Figure 3. Example of smartphone used during acquisition.

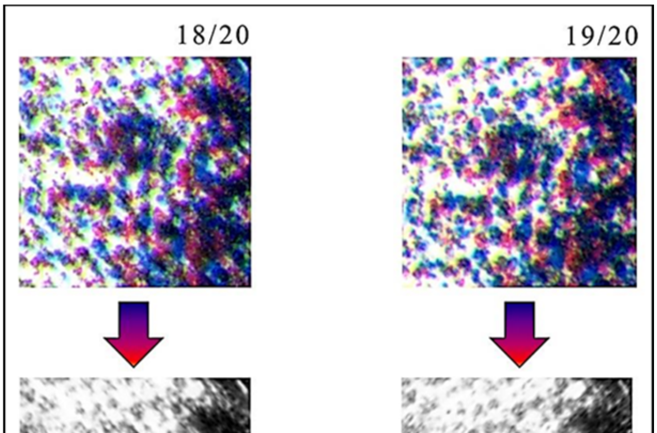

Figure 4. Hylemetric Hash Pattern of the Stone Lithography Dog 18/20 and Dog 19/20.

Starting from the obtained pattern, the proposed authentication system wants to introduce a new digital certificate of authenticity, uniquely connected with a specific lithography using the pattern itself.

The author (or the certification authority) decides which part of the artwork has to be acquired. This is acquired at High Definition; in this way it is possible to extract the related hylemetric pattern. This is sent, with the artwork information and the author digital signature, to the ADA server. The ADA software generates a unique artwork identification number and a dedicated Universal Resource Locator (URL), where the Digital Certificate is deployed. This process is similar to the digital object identifier (DOI) schema, as defined before in Section 2. A Metadata file about the object is stored in association with the DOI name and this file may include a location, such as a URL, where the object can be found.

The DOI to be used for retrieving artwork authentication and bibliographical information can be stored in a secure way inside an RFID. In the following section the complete system and the security introduced by RFID approach will be clearly explained.

4. SAFEART SYSTEM

RFID has considerable potential in product authentication. To resist against cloning and forgery are the most important security properties of authentication tags.

In RFID Product Authentication Techniques many ways are achievable to conduct a cloning attack. These include side channel attack [20], reverse-engineering and cryptanalysis [21], brute-force attack [22], physical attacks [23] and different active attacks against the tag [24]. In addition, shared secrets based product authentication approaches are always vulnerable to data theft, where the secret PIN codes or encryption schemes of valid products are stolen or sold out by insiders, which would enable criminals to create phony tags. This scenario is especially interesting for adversaries, because it would allow them to clone a large number of tags. Instead of fighting against cloning, it is possible using a different approach. In this approach, the authentication is based on writing on the tag memory a digital signature that combines the identification number and product specific random non cloneable features. In particular, artworks, due to the way in which they are produced, have an intrinsic randomness, due to the hand-made process. For painting, these can be the surface texture or a high resolution photo of a small piece of the painting.

If we refer to the oil painting reported in Figure 5, just for example, the acquisition and hylemetric pattern (i.e. hylemetric template) creation leads to a speckle-like appearance (the same analysis can be made also for lithography in Figure 4 obtaining a similar speckle pattern template). To avoid copy attack, duplication/replacement of the template file, the use of a digital signature is necessary. Digital signature grants that a document (in this paper the template constructed from the interested area) is original (i.e. constructed by the artwork author or by the certifier authority) and links the identity of the underwriter with the file and provides an official stamp (unalterable otherwise the digital signature verification fails) which legally determines the author of the document. In other words, the authentication template (speckle-like structure) T_C is digital signed by the asymmetric key algorithm [15], an encrypting "two keys system", which exploits devices able to produce two different,

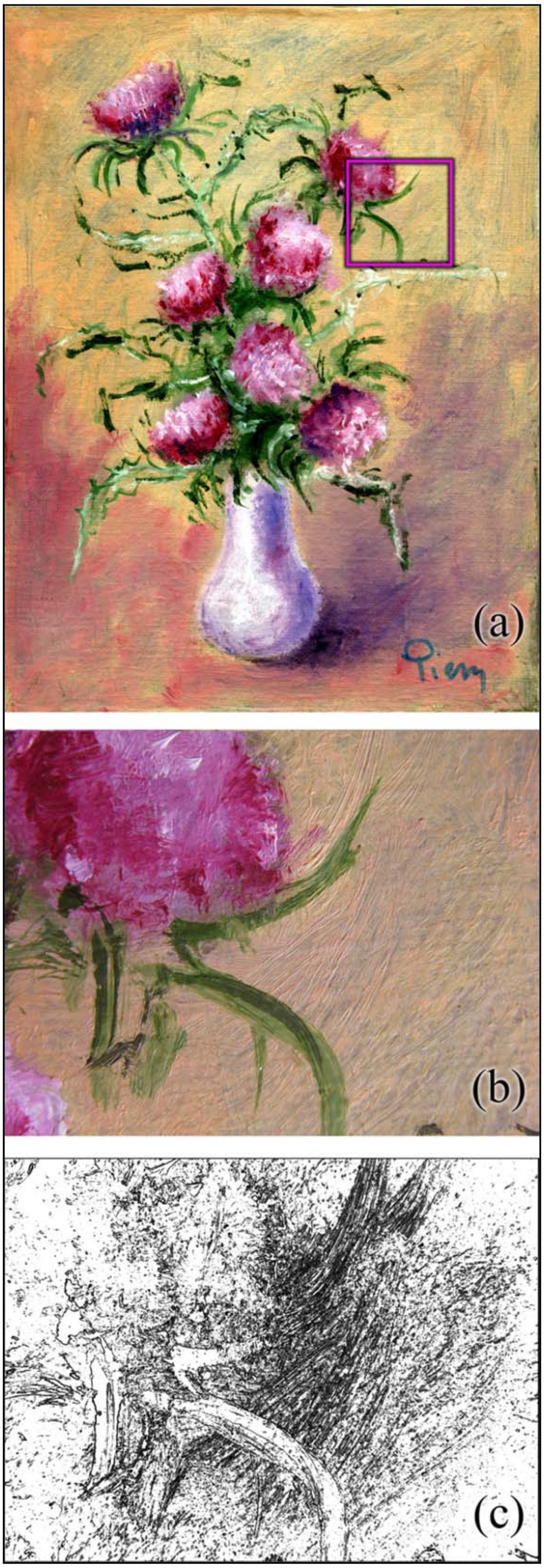

Figure 5. (a) oil painting with authentication area; (b) area acquired during verification phase; (c) Authentication Template.

but linked to each other, keys, one private (internal to the device and irretrievable) and the other public.

During the verification phase, the verifier can read the RFID, obtain the DOI with the related ADA URL, and retrieve the related public key. At this point, the verifier, from the RFID has also obtained the encrypted version of the hylemetric template, which could be decrypted using the obtained public key so it is possible having T_C^* ; in this way the data present in the certification media cannot be used for copy attack.

During the authentication phase the verifier captures an image similar to the one used to create the authentication template (T_T). In order to extract a vector to compare with that stored in the RFID, it is necessary to correct any possible distortion and acquisition error before calculating the template related to the test image to be used for verifying the painting authenticity. Using an automatic image registration algorithm [25], it is possible to obtain an “adjusted” image usable to extract the verification template.

Obviously, the captured image has residual geometrical distortion noise, which can lead to obtain a template different in comparison to that present in the authenticity media, also in case of original artwork verification. Therefore, considering that the template has a casual structure to allow the comparison between the calculated template and the authentication one retrieved from the RFID, a verification approach based on digital phase correlation calculation is proposed in this paper, similar to the one used in speckle field measurement [26].

In this work, the used Fourier-based phase correlation is:

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

In (1), Δx and Δy are the correlation peak coordinates, and are forward and backward Fourier Transform operators, respectively, and * means the complex conjugate. The coefficient α controls the correlation peak width. Optimum values range are from $\alpha=0$ for images characterized by high spatial frequency content and high noise level, to $\alpha=0.5$ for low noise images with less fine structure. For values greater than 0.5 the high frequency noise is magnified. In our experiment we have always used $\alpha=0.5$ values, also in case of noisy test images, obtaining in any case good results.

As in fingerprint approach, also in our procedure we introduce a correlation threshold, necessary to define if the two templates are similar enough to be considered as the same. Figure 4 shows the previously described process.

5. CONCLUSIONS

In this paper we presented an innovative system for verifying painting and drawing authenticity (and artwork in general), based on smartphone application, smartphone internal optical sensor (corrected with external macro lens, if necessary) and RFID tags. In addition to the stand-alone solution, also a web-based one is presented, to cope with RFID lifetime problems. The proposed solution can be used by living authors who want to protect their artworks from fraudulent copies marketed by dishonest sellers. Furthermore, the system can be used by foundations that deal with the protection of an artist. As well as from museum or large collection owners, for both certifying artworks authenticity and cataloguing them in an easy and secure way. In the further a deep analysis of limitations using NFC (Near Field Communication) reader instead of RFID ones will be presented, for better understating the optimum solution for non-contact artwork verification based on analogue fingerprint.

REFERENCES

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

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

[3] L. Cozzella, G. Schirripa Spagnolo, F. Leccese, Biometric-Like Approach for Verifying Artworks Authenticity, Applied Physics Research, 2013, 5(6), 118-130; http://dx.doi.org/10.5539/apr.v5n6p118

[4] M. Langston, J. Tyler, Linking to journal articles in an online teaching environment: The persistent link, DOI, and OpenURL, the Internet and Higher Education, 2004, 7(1), 51–58; http://dx.doi.org/10.1016/j.iheduc.2003.11.004

[5] G. Schirripa Spagnolo, L. Cozzella and D. Papalillo, Smartphone Sensors for Stone Lithography Authentication, Sensors 2014, 14, 8217-8234; http://dx.doi.org/10.3390/s140508217

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

[7] R. D. Melen, Record Document Authentication by Microscopic Grain Structure and Methods, US Patent US5325167 A, 1999; Available online: http://www.google.com/patents/US5325167, Last Accessed 02/14/2015

[8] J. Buchanan, R.P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D.A. Allwood, M.T. Bryan, Fingerprinting’ documents and packaging. Nature, 2005, 436; http://dx.doi.org/10.1038/436475a

[9] R.P. Cowburn, Laser surface authentication—Reading Nature’s own security code, Contempor. Phys. 2008, 49, 331−342; http://dx.doi.org/10.1080/00107510802583948

[10] B. Glover and H. Bhatt, 2006. RFID essentials. O'Reilly Media, Inc., Sebastopol (CA, USA), 2006, ISBN 0-596-00944-5

[11] K. Finkenzeller, “RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification”, Second Edition, John Wiley & Sons Ltd: Hoboken, New Jersey, USA, 2003, ISBN: 9780470844021

[12] I.K. Ibrahim, “Handbook of Research on Mobile Multimedia”, Information Science Reference, Hershey, New York – USA, 2008, ISBN 978-1-60566-046-2

[13] A. Laurie, Practical attacks against RFID, Network Security, 2007, 9, 4-1; http://dx.doi.org/10.1016/S1353-4858(07)70080-6

[14] European Digital Rights, Cloning an electronic passport, EDRI-gram, digital civil rights in Europe, 2006, No. 4–16. Available online: http://history.edri.org/edrigram/number4.16/epassport, Last Accessed 02/14/2015

[15] FIPS (Federal Information Processing Standards). Digital Signature Standard (DSS) 2013, PUB 186−4; http://dx.doi.org/10.6028/NIST.FIPS.186-4

[16] M. Langston, J. Tyler, Linking to journal articles in an online teaching environment: The persistent link, DOI, and OpenURL. Internet High. Educ. 2004, 7, 51–58; http://dx.doi.org 10.1016/j.iheduc.2003.11.004

[17] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J.A. Halderman, E.W. Felten “Fingerprinting Blank Paper Using Commodity Scanners”, SP 2009 - Proceedings of 30th IEEE Symposium on Security and Privacy, 301-314. http://dx.doi.org/10.1109/SP.2009.7

[18] C. Stein, C. Nickel, C. Busch, Fingerphoto Recognition with

Smartphone Cameras. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6-7 September 2012 , pp. 1−12. Available online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6313540, Last Accessed 02/14/2015.

[19] C. Connolly, T. Fliess, A Study of Efficiency and Accuracy in the Transformation from RGB to CIELAB Color Space, IEEE Trans. Image Process. 1997, 6, 1046−1048, http://dx.doi.org/10.1109/83.597279

[20] M. C. O'Connor, EPC Tags Subject to Phone Attacks, RFID Journal February 24, 2006. Available online: http://www.rfidjournal.com/articles/view?2167, Last Accessed 02/14/2015.

[21] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin and M. Szydlo, Security analysis of a cryptographically enabled RFID device, 14th USENIX Security Symposium, Baltimore, MD, 2005, Available online at the URL: https://www.usenix.org/legacy/events/sec05/tech/bono/bono.pdf, Last Accessed 02/14/2015

[22] A. Juels, RFID Security and Privacy A Research Survey, IEEE Journal on Selected Areas in Communications, 2006, 24(2), 381 – 394; http://dx.doi.org/10.1109/JSAC.2005.861395

[23] S. Weingart, “Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defense” , in Cryptographic Hardware and Embedded Systems — CHES 2000 Lecture Notes in Computer Science Volume 1965, 2000, pp 302-317 Proceedings of CHES'00, volume 1965 of Lecture Notes in Computer Science, pp. 302—317; http://dx.doi.org/10.1007/3-540-44499-8_24

[24] H. Gilbert, M. Robshaw, and H. Sibert, (2005). An active attack against HB+ – a provably secure lightweight authentication protocol. Electronics Letters, 2005, 41(21), 1169 – 1170; http://dx.doi.org/10.1049/el:20052622

[25] B. Zitová, J. Flusser, Image registration methods: a survey. Image and Vision Computing 2003, 21(11), 977–1000; http://dx.doi.org/10.1016/S0262-8856(03)00137-9

[26] M. Sjödahl, “Digital speckle photography Trends” in Optical Non-destructive Testing and Inspection, P. K. Rastogi and D. Inaudi (editors). Elsevier Publishing, Amsterdam, 2000, ISBN 9780080430201, pp. 179-195.