20th IMEKO TC4 International Symposium and
18th International Workshop on ADC Modelling and Testing
Research on Electric and Electronic Measurement for the Economic Upturn
Benevento, Italy, September 15-17, 2014

Analogue Fingerprinting for painting authentication

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, giuseppe.schirripaspagnolo@uniroma3.it, lorenzo.cozzella@uniroma3.it*
[2] *Università Roma Tre – Dipartimento di Scienze, address, maurizio.caciotta@uniroma3.it*
[3] *Expert in protecting cultural heritage, address, gianlucaferrari@gmail.com*

***Abstract* – Artwork counterfeiting is a wide problem in the art market, both for private subject and museums. In this paper an innovative system based on smartphone acquisition and mobile application is depicted to verify artwork authenticity based on random intrinsic object characteristics. This approach is based on biometry paradigm (analogue fingerprinting). The paper present a stand-alone solution, and an internet-based one, necessary for granting security verification also in case of problem with the used RFID tag. The proposed method uses an RFID Tag and a 2D barcode, in conjunction with an Internet-based Authentication Archive.**

I. 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 money amount 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, is necessary to consult the Museum archive.

For private collections or works produced by living artist, we must 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 himself near the item and so on. In other words, an identity documents is created and a unique set of fingerprints have 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 RFID tag with a high memory capacity, all (or part of) the information contained in identity document can be duplicated in the chip bonded on the artwork.

The rest of this paper is structured as follows: Section II outlines RFID tags. Section III defines the artworks fingerprints. Section IV defines the safeart system. Finally, Section V concludes the paper.

II. RFID SYSTEM

Radio Frequency IDentification (RFID) is a technology

ISBN-14: 978-92-990073-2-7

that allows a small radio device attached to an item to carry an identity for that item [5]. 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 [6].

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 a artworks (example: sandwiched between painting layers).

RFID is a wireless/contactless technology, avoiding remote manipulations, requires special protection service and risk management. 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) [7]. Due to many possible uses of RFID, there are a lot of differences in its systems components: different types of tags as well as variety of readers.

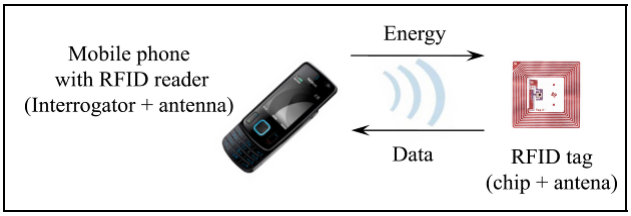

Fig. 1. The mobile device as part of the RFID system.

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 own data message. The reader decodes 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 [8], 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 [9].

In this paper, the problem of possible cloning of the RFID is not important. Authentication is done with the information contained into a RFID and robustness to 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 [10]. Digital signature grants that a document is original; in 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.

Figure 2 shows the Schema showing the artworks authentication step.

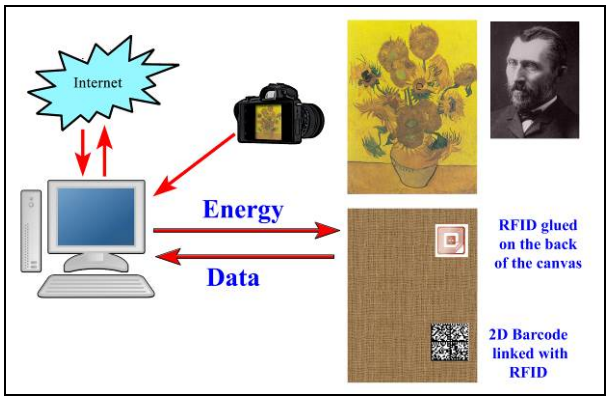

Fig. 2. Authentication Schema.

A possible stand-alone solution is based on using only a new generation smartphone and the info 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 verification phase. A dedicated application running on the smartphone can now acquiring the

requested area at high resolution, applying image corrections and locally calculating the template on the basis of patterns obtained from the high resolution image. Eventually a threshold-based correlation can be applied to verify if the two templates are as equal as necessary to be considered related to the same artwork.

The presence of a template digitally signed in the RFID, request to the verification application to known the public key of that template, for extracting the "readable" version to be compared with the locally calculated one. This step grants against the copy attack, where a 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 solution, 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 passive one, cannot be compared with 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.

III. FINGERPRINTING

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

- Universal: all the 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 present 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 proprieties must to have the technique used for authenticating the inanimate objects. In particular, in the artworks authentication the sampled characteristic should have the following properties [11]:

- Uniqueness: every object should be identifiable and distinguishable from all others;
- Consistency: feature vector should be verifiable by multiple parties over the lifetime of the object;
- Conciseness: 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 hylemetric characteristics 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 of exact or near-exact replication of the unique and random physical structure used as hylemetric characteristic has to be greater of 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.

IV. SAFEART SYSTEM

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

In RFID Product Authentication Techniques are achievable many ways to conduct a cloning attack. These include side channel attack [12], reverse-engineering and cryptanalysis [13], brute-force attack [14], physical attacks [15] and different active attacks against the tag [16]. 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 on 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.

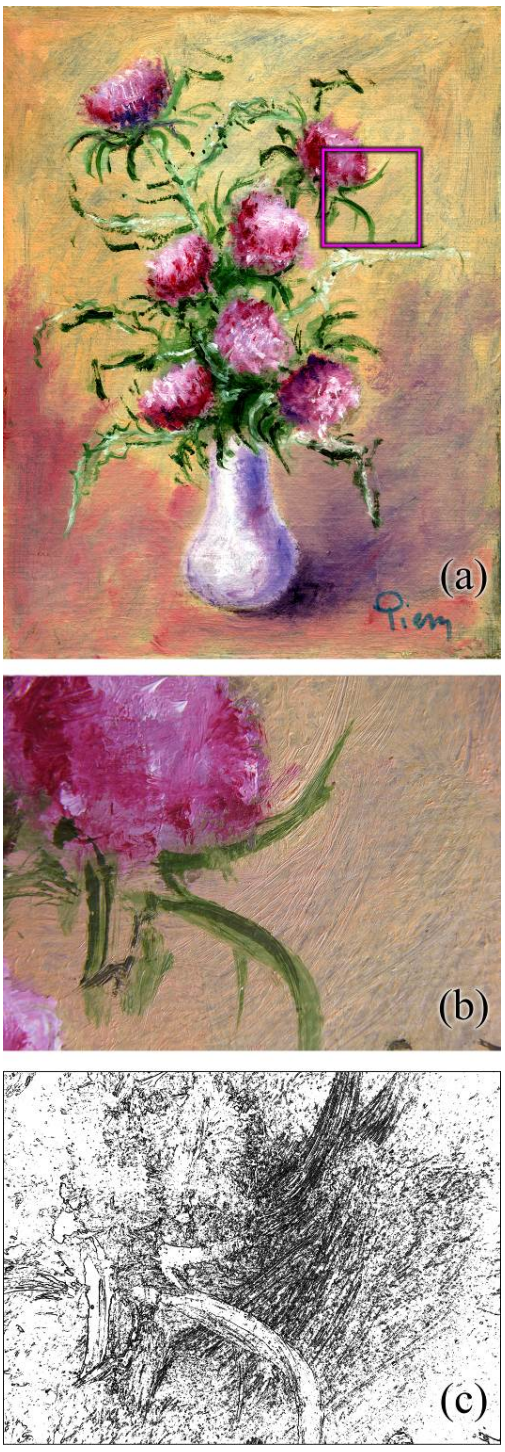

Fig. 3. (a) oil painting with authentication area; (b) area acquired during verification phase; (c) Authentication Template.

If we refer, to oil paint reported in Fig. 3(a), in our authentication approach, the first step is identifying an acquisition area (Fig. 3(b)). The next step is the creation of an authentication template, based on the acquisition of the interested area. In the reported example, the template is carrying out with a grey-leveling, high pass filtering, normalization, and subsequent thresholding (see Fig. (c)). The result has a speckle-like appearance.

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 asymmetric key algorithm [17], an encrypting "two keys system", which exploits devices able to produce two different, but linked each other, keys, one private (internal to the device and irretrievable) and the other public.

During the verification phase, by means of public Key, we obtain T_C from the encrypted T_C^*; in this way the data present in the certification media cannot be used for copy attack. Obviously, for verifying the painting originality, it is necessary decrypting the encoded image, using the associated public key.

During 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 relate to the test image to be used for verifying the painting authenticity.

Without a geometrical correction, could be possible that the verifier obtain a false negative result (i.e. false painting result in case of original one tested). To mitigate this situation, the next step in the proposed procedure is the application of Image Registration [18]. Image Registration will be able to make the corrections of scale, compensate the roto-translations and mitigate optical distortions. By means of image Registration we obtain an "adjusted" image usable to extract the verification template.

Obviously, the captured image has residual geometrical distortion noise, which can lead to obtain 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 among calculated template and the authentication one retrieved from the RFID, in this paper a verification approach based on digital phase correlation calculation is proposed, similar to the one used in speckle field measurement [19].

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

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

In Eq. (1) (Δx, Δy) are the correlation peak coordinates, and F and F^{-1} 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 image characterized by high spatial frequency content and high noise level, to $\alpha = 0.5$ 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 $\alpha = 0.5$ 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 the same. Figure 4 shows the previously described process.

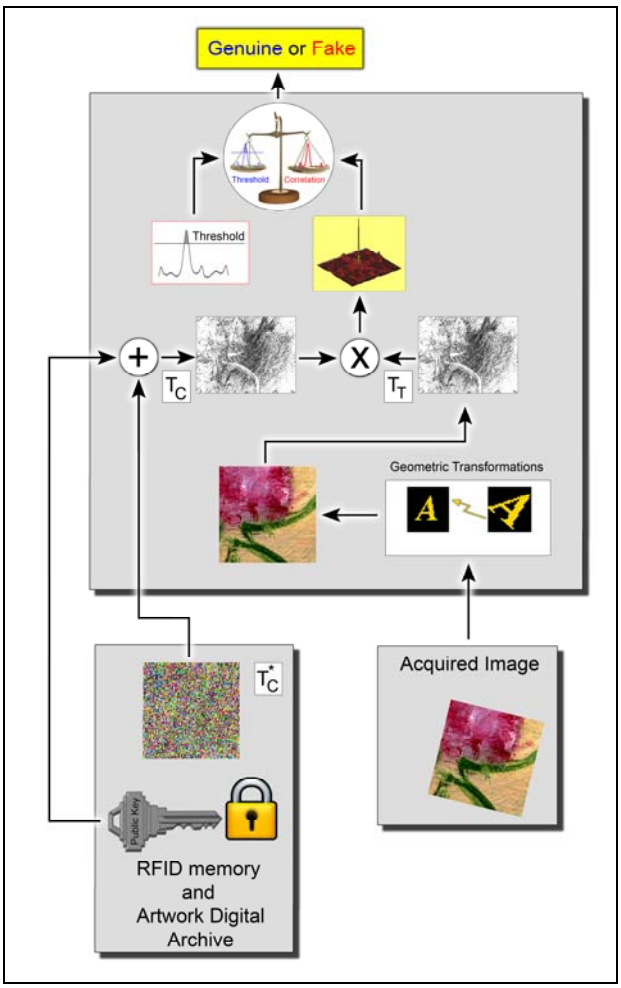

Fig. 4. Schema showing the authentication step. In the figure not all information stored in RFID are reported for easy understanding.

V. CONCLUSION

In this paper we have presented an innovative system for verifying painting and drawing authenticity (and artwork in general), based on smartphone application, smartphone internal 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 problem. 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 catalogue them in an easy and secure way. In the further a deep analysis of limitation using NFC 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, No. 6; 2013. http://dx.doi.org/10.5539/apr.v5n6p118

[4] M. Langston, J. Tyler, J "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] Glover, B., and Bhatt, H. 2006. RFID essentials. Sebastopol (CA): O'Reilly.

[6] 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

[7] Nokia international site. Images retrieved February 2, 2009. Available online: www.nokia.com

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

[9] European Digital Rights (EDRI-gram) (2006). Cloning an electronic passport. EDRI-gram, digital civil rights in Europe. No. 4–16. Available online: http://www.edri.org/edrigram/number4.16/epassport/

[10] FIPS (Federal Information Processing Standards). Digital Signature Standard (DSS) 2013, PUB 186−4. Available online: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[11] 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.

[12] RFID Journal (2006). EPC Tags Subject to Phone Attacks. News Article, February 24, 2006. Available online: http://www.rfidjournal.com/article/articleview/2167/1/1/ (4.5.2006).

[13] Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., and Szydlo, M. (2005). Security analysis of a cryptographically enabled RFID device. Preprint. Available online: www.rfidanalysis.org (4.5.2006).

[14] RFID Journal (2003). RFID, Privacy and Corporate Data. Feature Article, June 2, 2003. Available online: http://www.rfidjournal.com on subscription basis.

[15] S. Weingart, (2000). Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defense. In Cetin Kaya Koc and Christof Paar, editors, Proceedings of CHES'00, volume 1965 of Lecture Notes in Computer Science, pages 302--317. Springer-Verlag, 2000.

[16] H. Gilbert, M. Robshaw, and H. Sibert, (2005). An active attack against HB+ – a provably secure lightweight authentication protocol. Manuscript, July 2005.

[17] FIPS (Federal Information Processing Standards). Digital Signature Standard (DSS) 2013, PUB 186−4. Available online: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[18] 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

[19] Sjödahl, M. 2000 Digital speckle photography *Trends in Optical Non-destructive Testing and Inspection* 179-195 (Amsterdam: Elsevier Publishing)