Vision Security – the role of imaging for observer and observed

Marius Pedersen, Jon Yngve Hardeberg, and Christoph Busch
Gjøvik University College, Gjøvik, Norway

Abstract

Vision Security is the topic area that covers the intersection of Security with the human, who is the observed or the observing data subject, and who is most commonly the final user, customer or beneficiary of Security. For humans, the visual system is the main channel through which we receive information. The complex interplay between a human's perception of security and the associated trust in the system, and the actual digital components of security, opens a new and exciting topic area for imaging and imaging related problems. We focus in this paper on three areas; security and the perception of security, forensics, and biometrics.

Introduction

Security is of tantamount importance in our society, since security builds trust in the value of an item, in its originality and its integrity. Thus, security has direct and important applications in commerce, in contracts, the arts, cultural heritage, etc. Virtually in all areas of human interaction, trust is an essential component.

In the digital age, a whole new set of security problems came into existence and there is a considerable amount of work in digital security. What has been often overlooked, however, is the boundary line between the digital and human components of a system and this boundary line – we call it Vision Security – is where color imaging plays an essential role.

Without imaging, the secured data would be an abstract entity that does not fulfill its purpose in the interaction, imaging is what ties together the digital and human sides of security.

The role of imaging is crossing the boundary lines in both directions. On one hand, the digital system can learn from the human and from the human visual system to perform tasks that are very hard for a computer, but are seemingly easy for any human. On the other hand, imaging serves as the bridge that conveys both information and security&trust from the digital side to the human user.

Security and the Perception of Security

One everyday example of the difference in value and perceived value, as well as the difference in security and perceived security is common paper currency. The days of a "money" having an actual intrinsic value, as it had (and still has) with, for example, gold coins, are long gone, with most countries abandoning, or effectively abandoning the Gold Standard around the time of the first World War [1].

As described by Masuda et al. [2], a €100 note when used as tissue paper, would have an intrinsic or "use value" of less than a cent. Even adding the manufacturing cost to the use value wold only increase the total value to a few cent [3]. For example, a €100 note is produced at roughly €0.07 (note the date of reference [3]). The only reason we associate the higher value of €100 with that note is that other people around us are willing to exchange goods and services worth €100 with us for the possession of the note. It is the trust of the interacting parties in the system and in each other that establishes the reality of the face value. For that reason alone - not withstanding other reasons - individual countries and governments invest a serious effort in maintaining the trust by punishing counterfeiting or other manipulations of the value and trust.

A part of this equation is the actual trust we put in the authenticity of the note. A different piece of paper with the same "claimed" face value might not give us the same trust if there is something that does not seem right. And here, it is our visual system that often gives us the first indication and that works as a warning mechanism creating suspicion. As Masuda stated "Confidence in currency is a subjective matter of people's trust in banknotes"[2]. But what relates the confidence and trust? A very technical hypothesis would be that some objective metric, like number of security features inside the note, would be the best indicator for the confidence people have in the value. However, when looking at the correlation between "trust" expressed as a ranking of the difficulty to counterfeit a banknote, the respondents showed a low correlation between their assessment and the number of actual security features (known to the authors of the study) contained in the various banknotes from different countries. This is shown in Figure 1.

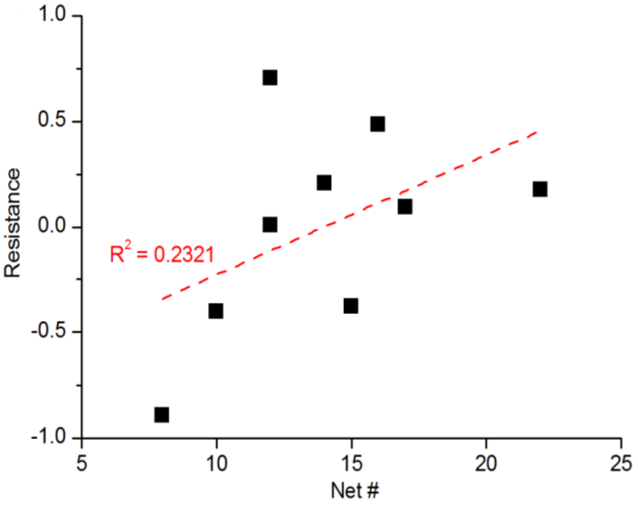

FIGURE 1: CORRELATION BETWEEN ASSESSMENT AND ACTUAL NUMBER OF SECURITY FEATURES.

The situation changes considerably, when we display the correlation between the observer assessment and the number of security features noticed by the same observer (Figure 2). In this case, a high correlation degree was obtained (an R2=0.8769 up from R2=0.2321).

Figure 2 strongly suggests that "what we see" is what influences our assessment of security in a powerful way.

This is exactly the overlap between Vision and Security that we mentioned in the beginning. Without a deep understanding of the human and human visual system we will be very inefficient in creating and using Security in a manner that is effective against attack and at the same time effective in generating the required trust from the user.

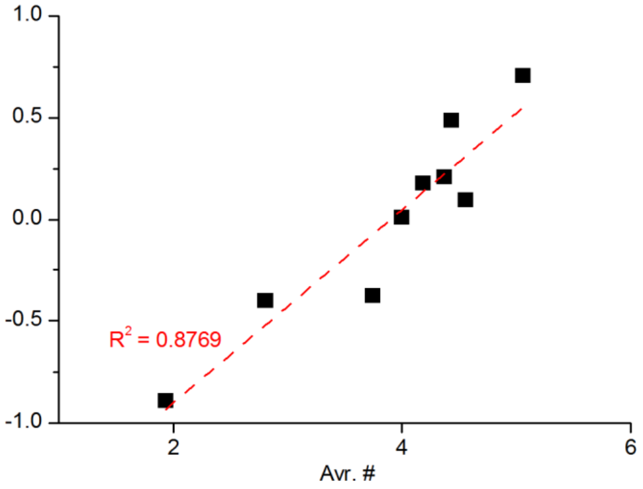

FIGURE 2: CORRELATION OF ASSESSMENT AND RECOGNIZED SECURITY FEATURES

Forensics

The previous section discussed the role of human vision in the creation of trust. In this section, we will examine the role of imaging science in the examination of images for various purposes, commonly referred to as "forensics".

The use of imaging has a long history for security applications, the first record of using photography for forensic purposes dates back to around 1840[4]. Manipulations of images began shortly thereafter, and since 1850 extensive tampering of images has occurred.

Forensics faces a number of challenges and demands[5]. Tiny pieces of evidence, chaotic environment, abnormalities, partial knowledge and uncertainties are considered as challenges, and sufficient quality of trace evidence, objective measurement, robustness & reproducibility, and secure against falsification as demands.

In forensics the complete digital image life cycle can be used to identify the source of the image or to determine whether the content is authentic or modified [6]. Commonly, three main parts are considered: image acquisition, image coding, and image editing. Historically, from image acquisition traces left by the optics, the sensor, and the Color Filter Array (CFA) have been used for image forensics. Since then, image acquisition is also performed with scanners, and many of the methods developed for cameras have also been applied to scanned images [7].

An acquisition device model presents individual lens characteristics; and in the past chromatic aberration [8] and spherical aberrations[9] have been investigated. Present techniques for chromatic aberrations even go so far as to distinguish different copies of the same lens [10]. In the technique by Yu et al. [10] a white noise pattern image was used, with the advantage of solving the pattern misalignment problem. The white noise pattern also eliminates the instability of corner detection. Their experiments show that the lens focal distance is important for the shaping lens chromatic aberration pattern, and by fixing the focal distance a stable chromatic aberration pattern can be obtained. A recent technique [11] has also shown that it is possible to use Purple Fringing Aberration for forensics purposes, where inconsistencies in the direction of the fringing are used for tampering detection.

Information from the sensor has also been field of interest for the forensic community. Information about dead pixels [12] and sensor noise have been used to detect tampering. Lukás et al. [13] used information on sensor noise in terms of the blockwise correlation between the estimated photoresponse nonuniformity noise and an image to detect tampering.

Knowledge and understanding of the CFA is valuable in forensics. Interpolation of the CFA results in specific statistical correlations between a subset of pixels in each color channel [14]. Since the color filters in a CFA are typically arranged in a periodic pattern, these correlations are periodic. In addition, it is unlikely that recorded pixels will have the same periodic correlation. This makes it possible to use the correlations as a signature for image forensics. Popescu and Farid [15] proposed a statistical approach to image authentication based on the CFA correlations, in which they use a two-step iterative expectation-maximization algorithm

Bayram et al. [16] proposed a method for camera identification based on traces of color interpolation in the RGB color channels. A number of measures was found using the expectation-maximization algorithm from Popescu and Farid [17] , further a SVM classifier was designed and used to decide how well the selected measures could classify images from different cameras.

Form the aforementioned work, it is clear that imaging has played and will play an important role in the forensic part of security and with the fast advances of digital imaging, this part will likely increase rather than decrease with time.

Biometrics: Trusting the Data

For more than a hundred years, criminal investigators have been using fingerprints to catch suspects on the basis of evidence at the scene of the crime. Today, computers have automated identification and compare evidence found at the scene of a crime with millions of stored fingerprint images in just a few seconds. But in addition to fingerprints, facial and iris images can be used as means of identification in a biometric process. It is no longer just criminal investigation offices that apply these technologies - many commercial access control systems are now using biometrics for identification purposes. Biometrics, which is understood as the automated recognition of individuals based on their behavioral and biological characteristics, exploits the rich set of anatomical characteristics related to the structure of the body (finger pattern, iris pattern etc.). These characteristics can be measured more or less directly. Vision based biometric capture devices (facial sensor, iris sensor) are non-intrusive and widely acceptable, additionally, the security system also relies on integrity of the recorded data (as in the previous forensic case). Moreover it also relies on the trust, that the capture device can reliably distinguish a normal presentation from a genuine data subject on one side, from an artifact that is presented to the capture device with the intention to impersonate an enrolled data subject. Such an artifact could be a simple instrument such as printed photo, electronic display that is replaying a video, a physical imitation [18] or a complete three-dimensional facial mask. Such attacks on the capture device need to be tackled with Presentation Attack Detection (PAD) algorithms, which are also known as anti-spoofing methods [19][20]. In the first line of defense the capture device must be capable to distinguish a flat presented artifact object (i.e. the photo print out) from a 3D facial surface, which is attributed to an authorized genuine subject. However in order to detect severe active imposter attacks such as the 3D-facial mask [21], things are getting more complicated. Beyond that we must consider concealer presentation attacks for which a data subject (likely known to the system) mitigates or mutilates his facial surface with the intention to evade being recognized by the system [22][23][24].

While we can assume trust in the capture device once the PAD-challenge is solved, a biometric system with its intrinsic goal to recognize data subject, even after a long time period after the enrollment procedure, must also ensure the quality of samples processed in the system. Quality of data that is input to feature extraction and machine learning systems is of utmost importance for the benefit of machine-based expert system. The established saying "garbage in – garbage out" is well underlining the fact that helpful support of an expert system can only be expected, if the quality of data in the operational use is under control. At the same time humans that interact with computer based expert systems can only trust the machine, if the computing system is reliable in the sense that it is robust against variance or even outliers in the data and can always provide a meaningful response. For Vision Security that is serving our target applications (e.g. Biometric Access Control) the research questions also attempt to formulate data quality and method reliability metrics that reflect human expert knowledge [25].

The issue of quality control of captured data reaches out into our home and mobile environment. If for instance smart phones are used as mobile imaging components, then a reliable system must control the level of compression that is applicable to video, in order to accelerate processing the footage at no loss of service quality. As an example for said biometric applications we need also to assure that we can accurately assess and control the quality of images that are enrolled in the systems database. A prerequisite to do so is obviously to identify sensor, human interaction and environmental factors that have an impact on the quality of captured data, and to model them subsequently. The intention in this case is to research and evaluate quality measures and assess how reliable these measures can predict the accuracy of the security system [26] (i.e. the biometric recognition). Once that problem will be solved such measurement can help improving biometric system accuracy and efficiency during the capture process (as a control-loop variable to initiate re-capture decisions, if needed), in database maintenance (sample update), in enterprise-wide quality assurance surveying (to initiate training) and in invocation of quality-directed processing of samples in multimodal systems. Biometric quality analysis is a long-term technical challenge because it is most helpful when the quality measures reflect the performance sensitivities of one or more target biometric comparison subsystems. Further as humans are the ones that benefit from expert systems (and security systems), they must at all times remain well informed about the strength of defense mechanisms that are incorporated in the security system.

Summary

Vision Security is a new look at the intersection of Security Systems and the Human User. In this interaction, imaging plays an important role, both in the sense that imaging is needed to communicate with the humans, as well as in the area of learning and off-loading from the human.

Without imaging, secured data would be an abstract entity that does not fulfill its purpose in the interaction, imaging is what ties together the digital side and the human side of security. Without learning from the human, many security tasks would be difficult to accomplish.

The role of imaging is crossing the boundary lines in both directions. As such it is an important bridge and the problems associated with being this bridge establish a new area in imaging which we call Vision Security.

References

[1] See for example: https://en.wikipedia.org/wiki/Gold_standard

[2] O. Masuda et al. ,"Effects of awareness to security features on the confidence in banknotes", J. Print Media Technol. Res. 4(2015)2, 103–110

[3] de Heij, H.A.M., 2006. "Public feedback for better banknote design". In: van Renesse, R.L., ed. Proceedings of SPIE Vol. 6075, Optical Security and Counterfeit Deterrence Techniques VI. San Jose, CA. 17–19 January 2006

[4] H. L Blitzer, K. Stein-Ferguson, J. Huang Understanding Forensic Digital Imaging. Elsevier. 2008..

[5] Katrin Franke, Sargur N Srihari, "Computational forensics: An overview". Computational Forensics. 1-10. Springer Berlin Heidelberg. 2008.

[6] Piva, A.: An overview on image forensics. ISRN Signal Processing, 2013, 2013, article ID 496701

[7] G. Sharma et al., "Systems and methods for associating color profiles with a scanned input image using spatial attributes", US-A 7,474,783 (2009)

[8] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in Proceedings of the 8th workshop on Multimedia & Security, S. Voloshynovskiy, J. Dittmann, and J. J. Fridrich, Eds., pp. 48–55, ACM, Geneva, Switzerland, September 2006

[9] T.V. Lanh, K.-S. Chong, S. Emmanuel, M. Kankanhalli, A survey on image forensic methods, in: International Conference on Multimedia and Expo (ICME 2007), Beijing, China.

[10] Jun Yu ; Scott Craver ; Enping Li; Toward the identification of DSLR lenses by chromatic aberration. Proc. SPIE 7880, Media Watermarking, Security, and Forensics III, 788010 (February 10, 2011); doi:10.1117/12.872681.

[11] I. Yerushalmy and H. Hel-Or, "Digital image forgery detection based on lens and sensor aberration," International Journal of Computer Vision, vol. 92, no. 1, pp. 71–91, 2011.

[12] Z. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, "Methods for identification of images acquired with digital cameras," in Proc. Enabling Technologies for Law Enforcement and Security, Feb. 2001, vol. 4232, pp. 505–512

[13] J. Lukás, J. Fridrich, and M. Goljan, "Digital camera identification from sensor noise," IEEE Trans. Inform. Forensics Security, vol. 1, no. 2, pp. 205–214, 2006

[14] Farid, H., "Image forgery detection," *Signal Processing Magazine, IEEE* , vol.26, no.2, pp.16,25, March 2009

[15] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Trans. Signal Processing, vol. 53, no. 10, pp. 3948–3959, 2005.

[16] Bayram, S.; Sencar, H.; Memon, N.; Avcibas, I., "Source camera identification based on CFA interpolation," *Image Processing, 2005.*

ICIP 2005. IEEE International Conference on , vol.3, no., pp.III,69-72, 11-14 Sept. 2005

[17] A. Popescu and H. Farid, “Exposing Digital Forgeries by Detecting Traces of Re-sampling,” IEEE Transactions on Signal Processing , 2004.

[18] http://arstechnica.com/tech-policy/2013/03/brazilian-docs-fool-biometric-scanners-with-bag-full-of-fake-fingers/
also A. Zwiesele, A. Munde, C. Busch, H. Daum: "Comparative Study of Biometric Identification Systems" In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

[19] J.Galbally,S.Marcel,andJ.Fierrez.Imagequalityassessmentforfakebiometricdetection:Application to iris, fingerprint, and face recognition. *Image Processing, IEEE Transactions on*, 23(2):710–724, Feb 2014

[20] ISO/IEC JTC1 SC37 Biometrics. ISO/IEC IS 30107-1. Information Technology - Biometric presenta- tion attack detection - Part 1: Framework. International Organization for Standardization, 2015.

[21] 3D Face Mask. http://www.thatsmyface.com/, 2015

[22] R. Raghavendra and C. Busch. Novel presentation attack detection algorithm for face recognition system: Application to 3d face mask attack. In IEEE International Conference on Image Processing (ICIP), Paris, France, pages 323–327, Oct 2014.

[23] R. Raghavendra and C. Busch. Robust 2d/3d face mask presentation attack detection scheme by exploring multiple features and comparison score level fusion. In 17th International Conference on Information Fusion, FUSION 2014, Salamanca, Spain, pages 1–7, 2014.

[24] R. Raghavendra, K. Raja, and C. Busch. Presentation attack detection for face recognition using light field camera. IEEE Transactions on Image Processing, 24(3):1–16, 2015.

[25] M. Olsen, M. Böckeler, C. Busch: "Predicting Dactyloscopic Examiner Fingerprint Image Quality Assessments", in Proceedings of the IEEE 14th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 9-11, (2015)

[26] M. Olsen, V. Smida, C. Busch: "Finger Image Quality Assessment Features - Definitions and Evaluation ", in Journal on Biometrics, IET, (2015)