Image security and biometrics: A review.

Ion Marqués, Manuel Graña

Grupo de Inteligencia Computacional, UPV/EHU
www.ehu.es/ccwintco

Abstract. Imaging security and biometrics are two heavily connected areas. The quick evolution of biometrics has raised the need of securing biometric data. A majority of this data is visual, which has lead to intensive development of image security techniques for biometric applications. In this paper we give a fast fly over image security approaches and imaging-related biometrics. We present the current state-of-the-art of the interplay between both areas. The emphasis in this paper is the computational methods.

1 Introduction

Securing data is an important and evolving area of computer science. Text was the initial asset to be secured. Nowadays visual information is also present in computerized processes. Last years have seen an increasing interest on security methods for image data. The goals can be to ensure:

1. The *authenticity* and/or ownership of the image creator or sender.
2. The *integrity* of the image data, and the ability to know if the image has been altered.
3. *Privacy*, in terms of content and/or ownership of the data.

The developed methods must also usually compel *performance* requirements (speed, memory usage, etc.), *usability* criteria (user-friendliness, no expertise requirements,etc.) and other features that could be necessary. Some security techniques like watermarking and steganography have been present in imaging science for a long time. Adaptation of classic cryptography to image data has also been done. These areas have recently seen a boost in research interest due to the nature of the image data: Many biometric systems use imaging methods, and the need for secure biometrics storing and sharing schemes is increasing. Figure illustrates the interplay between these two areas.

This paper introduces the cited image security techniques in section 2, citing the most recent developments on the area. Section 3 gives an overview on image-based biometrics and presents how image security techniques are being applied to it. For lack of space we will obviate the conclusions section.

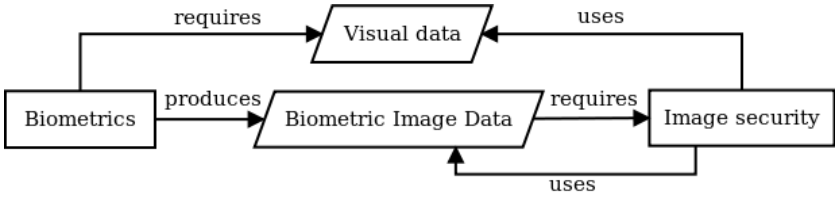

Fig. 1. A simple flowchart that illustrates the relation between biometrics and image security. Note that each arrow involves the use of computational methods.

2 Image security

Securing the storage and transmission of images is one of the cornerstones of data security. Communication protocols like Secure Sockets Layer (SSL) use Message Authentication Codes to guarantee the correct identities of the sender and receiver of data fragments over the Internet. Similarly, multimedia content such as audio, images or video can be object of authentication, integrity and data hiding procedures. The two main approaches to authentication on imaging science are watermarking and cryptography. The main difference between both methods is that Watermarking aims to introduce the signature of the owner without altering the visual perception of the data. Conversely, encrypted images are not readable without a decryption step. Most watermark methods and cryptosystems also seek data integrity. Image steganography could be seen as a special case of watermarking, where the goal is to hide information into the image.

2.1 Watermarking

The goal of watermarking is to embed data into an image by introducing changes which must comply three requirements: 1) To be imperceptible to the human eye 2) To be recoverable by a computer programs and 3) To be generated an embedded so that attackers can have access to it. These requirements and the nature of image data arise some properties that watermarking algorithms must suit [61,24]:

- Fidelity: The higher the fidelity the more difficult is to notice the watermark. This is not a computational feature, but a visual perception subjective measure.
- Capacity: This property corresponds to quantity of information that a watermark can hold.
- Robustness: The watermarking process should be resilient to passive distortion sources. This distortions can be caused by image processing, transmission distortion, and storage distortion. The robustness also corresponds to the ability of the watermarking to resist attacks like watermark removal, covert communication detection, collusion attacks or forgery attacks.

These properties can collide, so the watermarking process must have a proper tradeoff between them. Tremeau et al. gave a good example of these phenomenons [61]. In order to be robust, the watermark should be placed in the most significant parts of the data. In fact, many watermark removal attacks compromise the perceptually less significant components via compression. However, in order to retain a high fidelity, a watermark has to be placed in the less perceptually significant parts of the data. Therefore, robustness and fidelity are in conflict. Its important to know well the application domain of the watermarking process in order to find the right balance between these properties. These applications include [24]:

- Ownership assertion: The owner of an image can generate and embed a unique watermark. The user could make a watermark based on a private key. He or she can not only ensure his or her identity but also claim the ownership of the image, as he or she is the only one that knows the key.
- Data integrity: Any change made to the image will also affect the watermark.
- Fingerprinting: Transactional watermarks allow to link the image data to the receiver of the data. For instance, in a closed or secret media creation process, custom watermarks can help to identify the source of a possible leak. It can also be implemented a copy control system. Instead of preventing illegal copies watermarking can track the illegal activity. Media player and recorders can also be programmed to refuse copying protected material.

Many recent researches focus their goal to a specific domain of image data. Image forgery prevention is one of the areas. Although blind methods are broadly researched [47], watermarks are invaluable tools for image forensics. Other big interest is the copyright protection. Many algorithms are designed and tested for a specific video codec or image format [70]. Some applications, like medical imaging or arts storage require that the data cannot be modified -i.e. losses or lossy-to-lossles procedures. Other aspect affecting the development of watermarks is what to encode, for example a 2-Dimensional bar code [40] or a logo [62]. There is also a growing interest in fusing watermark-protected biometric data [65]. Besides well known 2 dimensional image and video watermarking, research on watermark insertion in 3 dimensional visual data is been also developed [67]. There has been wide interest in the use of computational intelligence methods for watermarking and are extensively revised in [25]. Some methods use a signal processing approaches like wavelet transforms [14] and Independent Component Analysis [50]. In this line of work, other researches propose fuzzy clustering approaches [22], genetic algorithms [37] or hybrid approaches [26,15]. As an extension of these methods, some researchers seek the capability of retrieving the watermark from the image, in order to test separately its authenticity [17,23]. It is also interesting the ability of not only detecting unwanted modifications but also recovering the original image [76].

2.2 Image Cryptography

The goal of encrypting images is to hide it's content from unauthorized viewers and authenticate its owner. Classic cryptography was centered on text data.

Nowadays, more research is being done focused on image data. The idea is to use the visual information as the different components that form a cryptosystem. Furthermore, it is desirable that the procedure does not require additional optical hardware [36]. For example, the amplitude distribution of the Hartley transform can be the public key and the phase distribution the private key [36]. Other similar approaches use Mellin transform [79], Fractional Fourier transform [78] or blind source separation algorithms [46].

Other aspect of cryptography applied to images is Visual Cryptography. The idea is to divide visual information into meaningless trunks and divide them between users. The image can only be reconstructed if all the parts are overlaid in a certain way, hopefully without loss of information [73,74,39]. This methods don't require keys because the human visual system decrypts the data. Visual Cryptography is closely related to Stenography, which is discussed in subsect. 2.3.

2.3 Information hiding on images

The science that involves hiding and communicating secret data in a multimedia carrier like images or video is called steganography. Its goal is to hide the very existence of the secret data. This is an key feature in applications like medical image sharing [64] which handle very private data. Cheddad et al. [19] published recently an exhaustive survey on image steganography. We will focus on the computational intelligence tools and the latest publications on the matter.

Most algorithms work on spatial [41,60] or frequency [13] domain. They make use of computational tools like predictors [63], particle swarm optimization [53] or fuzzy detectors [16]. Recently, adaptative algorithms are being developed, where more information about the image is used. The combination of statistical and frequency information with image object or texture knowledge can lead to better results [19]. Some of these approaches even try to enhance the quality of the image at the same time that they embed the data [69]. These techniques are obviously dependent on the image format and aren't usually designed for palette-based images [77].

3 dimensional models can also be subject to steganography. Previous hiding efforts for 3D models were usually modified watermarking techniques. Only since 2009 researchers have started to design 3D steganography algorithms. Chao et al. [18] proposed a multi-layered method. It had high capacity but was not secure against certain malicious attacks such as smoothing, additional noise, nonuniform scaling, simplification, and vertices resampling. In 2010 Amat et al. developed a losses algorithm in the sense that vertices's position was not altered [6]. Their method is based on minimum spanning trees. Other recent researches rely on 2D imaging techniques [28].

3 Biometrics and image security

The importance of image security is most notable in Biometrics. Biometrics consist on a series of methods for unequivocally recognizing a subject (typically

a human but can also be other animal). Biometric algorithms and procedures should conform a system which ensures the identity of the target using biological traits: Fingerprint, face image, DNA sequence, voice, walking gaits, etc. Many of these techniques are closely related to imaging science -see table 1. Some methods aim to identify one subject, while others require the verification of the person [58]. Most of biometric systems require strong security. Therefore, they usually make use of watermarking, cryptography and steganography. Biometric systems should have some properties by definition, and also some other issues that must be considered [38,1]:

- Universality: Applicable to every human.
- Distinctiveness: Any two subject's biometric features must be sufficiently distinguishable.
- Permanence: The biometric features should be persistent over time. Obtaining or verifying them should not induce changes in the user's biometric features.
- Collectability: The features can be measured quantitatively.
- Performance: Accuracy, speed, low resource usage and invariability to environmental factors are desirable.
- Acceptance: It is important to measure the social acceptance of a certain biometric characteristic.
- Security: Biometric systems should ensure authenticity, integrity, privacy and resistance to attacks and forgery.

Table 1. Summary of biometric methods and their relationship with imaging techniques. Note: EHF stands for Extremely High Frequency (30-300 GHz wavelength).

Technique	Image-based method? (image type)	Involvement of imaging techniques	
		Acquisition	Verification/identification
Face recognition	Yes (visual)	Yes	Yes
Ear recognition	Yes (visual)	Yes	Yes
Thermography	Yes (infrared)	Yes	Yes
Palmprint/fingerprint	Yes (scan)	Yes	Yes
Iris	Yes (visual)	Yes	Yes
Retinal scan	Yes (infrared)	Yes	Yes
Geometry (e.g. hand)	Yes (scan)	Yes	Yes
Gait	Yes (video)	Yes	Yes
EHF imaging (e.g thorax)	Yes (EHF)	Yes	Yes
Dental	Sometimes	Sometimes	Sometimes
Signature, keystroke	No	Sometimes	Sometimes
Voice	No	No	Sometimes
Odor	No	No	No
DNA	No	No	No

3.1 Imaging and biometrics

Face recognition [20] is one of the most relevant applications of image analysis. It is been widely proposed and used as a biometric feature. In fact, to build an automated system which equals human ability to recognize faces is one of the core challenges of biometrics. Face recognition may consist in the authentication of a user, which is a binary decision problem. Most commonly, it consists in the search for the identity of a subject in a large face database, which is a (large) multi-class problem. This initial problem can be extended to gaze, expression or mood recognition [59].

Recent researches on this topic have used classic approaches like finding optimal discriminant projections which seek to preserve locality [29] or supervised discriminant methods [66]. Other approach is not to select the optimal features but to have a sufficient number of them via sparsity preserving methods [54,68]. Frequency-based algorithms like wavelet transforms are also being used [75]. Although it has seen fewer interest lately, some researches seek to use anthropomorphic geometric features [56]. This approach is an example of what is known as Soft-biometrics. This branch of biometrics uses features "easy" to extract (like skin, eyes, or non-facial features like ethnicity). It can be useful to enhance "hard" face recognition biometric methods [49]. On a side note, the usefulness of infrared or near-infrared imaging for face recognition is still a open question [34] as the infrared signature of a face can change a lot through time. However, infrared information can help face recognition systems overcome pose, illumination and expression variations [52]. The use of 3D information is also being use to build systems invariant to those problems [27].

Unlike face recognition, iris scanners usually require an action by the subject. In other words, the user must come close to the iris scanner and stay still. One of the objectives of iris biometrics is to design less obtrusive acquisition procedures [12]. This is a limitation is an inconvenience for the user, but prevents problems like occlusion or poor image retrieval. Other advantage is that biometric systems differentiate between left and right eyes and between irises of identical twins [35]. On the other hand, iris biometrics face degradation problems caused by pupil dilation [33] or contact-lenses [9]. Other issue is the segmentation of the iris. An iris recognition system must extract the iris region and discard the pupil, eyelids, sclera, etc. Recent studies have achieved fast and accurate segmentation overcoming reflection problems [32]. The iris texture extraction step is performed using techniques like Discrete Cosine Transform, Fourier Transform, Faar wavelets, Gabor filters, etc. [43,12]. Santos et al. propose in [57] a fusion scheme to take advantage of different extraction techniques. They results show that fusing methods can lead to systems less sensitive to poor quality data. This contribution is relevant in terms of building systems less intrusive.

Other image-based biometric systems include fingerprint or palmprint recognition [7,21,42], hand geometry [51], dental biometrics [45], ear biometrics [8], millimetre-wave scans [3], etc.

Multi-modal biometrics is another current research area. The idea behind the multi-modal or hybrid biometrics is to combine different methods to optimize

the aspects listed on the beginning of sec. 3. Some researches develop statistical tools to effectively extract and fuse features from different sources, like face images and palmprint scans [71]. Other recent researches fuse the features at the score or classification level [72,48,5,31]. Computational tools like particle swarm optimization [55] are also being used to enhance the fusion step.

3.2 Biometric image security

Biometric data must be appropriately secured, but biometrics also offers a wide array of security applications (e.g. e-passport [58]). However, there are widespread security concerns regarding the stored biometric data. The use of biometric features like face images or fingerprints to enhance classic cryptographic or watermarking systems is a promising approach. This research subject open some concerns: What happens if the biometrics of a subject are stolen? What is the proper balance between performance and robustness? What biometric approach should we use in terms of proper universality, distinctiveness, social acceptance, etc.?

One of the approach is to secure biometric images via encryption techniques. These methods sometimes perform lossy procedures over the images [10,2]. Generally this systems must decrypt the data in order to proceed to the authentication process. The challenge of bio-cryptography is to implement *cancelable* biometrics [11], which can be described as the application of non-invertible and repeatable modifications to the original biometric templates.

Steganography [53] and watermarking [44,4] are also being employed on biometric data security. This technique allows embedding large amounts of biometric information within an image. Steganography can be employed to embed biometric images into publicly transmitted images [53]. Multimodal biometric image watermarking is also a promising research area [30,65].

References

1. Biometric technology today. volume 2011.
2. Bibhudendra Acharya, Mukul Dhar Sharma, Sourabh Tiwari, and Vinay Kumar Minz. Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem. *Procedia Computer Science*, 2(0):242 – 247, 2010.
3. B.G. Alefs, R.J.M. den Hollander, F.A. Nennie, E.H. van der Houwen, M. Bruijn, W. van der Mark, and J.C. Noordam. Thorax biometrics from millimetre-wave images. *Pattern Recognition Letters*, 31(15):2357 – 2363, 2010.
4. Mohamed Mostafa Abd Allah. Embedded biometric data for a secure authentication watermarking. In *Proceedings of the Fourth conference on IASTED International Conference: Signal Processing, Pattern Recognition, and Applications*, pages 191–196, Anaheim, CA, USA, 2007. ACTA Press.
5. Fawaz Alsaade, Aladdin Ariyaeeinia, Amit Malegaonkar, and Surosh Pillay. Qualitative fusion of normalised scores in multimodal biometrics. *Pattern Recognition Letters*, 30(5):564 – 569, 2009.

6. P. Amat, W. Puech, S. Druon, and J. P. Pedeboy. Lossless 3d steganography based on mst and connectivity modification. *Signal Processing-Image Communication*, 25(6):400–412, JUL 2010.
7. Gholamreza Amayeh, George Bebis, Ali Erol, and Mircea Nicolescu. Hand-based verification and identification using palm-finger segmentation and fusion. *Computer Vision and Image Understanding*, 113(4):477 – 501, 2009.
8. Banafshe Arbab-Zavar and Mark S. Nixon. On guided model-based analysis for ear biometrics. *Computer Vision and Image Understanding*, 115(4):487 – 502, 2011.
9. Sarah E. Baker, Amanda Hentz, Kevin W. Bowyer, and Patrick J. Flynn. Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. *Computer Vision and Image Understanding*, 114(9):1030 – 1044, 2010.
10. Gaurav Bhatnagar, Jonathan Wu, and Balasubramanian Raman. Fractional dual tree complex wavelet transform and its application to biometric security during communication and transmission. *Future Generation Computer Systems*, 28(1):254 – 267, 2012.
11. Ruud M. Bolle, Jonathan H. Connell, and Nalini K. Ratha. Biometric perils and patches. *Pattern Recognition*, 35(12):2727 – 2738, 2002.
12. Kevin W. Bowyer, Karen Hollingsworth, and Patrick J. Flynn. Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding*, 110(2):281 – 307, 2008.
13. Sofiane Braci, Claude Delpha, and Remy Boyer. How quantization based schemes can be used in image steganographic context. *Signal Processing-Image Communication*, 26(8-9):567–576, OCT 2011.
14. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. De Natale, and A. Neri. A commutative digital image watermarking and encryption method in the tree structured haar transform domain. *Signal Processing: Image Communication*, 26(1):1 – 12, 2011.
15. Chin-Chen Chang, Kuo-Nan Chen, Chin-Feng Lee, and Li-Jen Liu. A secure fragile watermarking scheme based on chaos-and-hamming code. *Journal of Systems and Software*, 84(9):1462 – 1470, 2011.
16. Chin-Chen Chang, Jung-San Lee, and T. Hoang Ngan Le. Hybrid wet paper coding mechanism for steganography employing n-indicator and fuzzy edge detector. *Digital Signal Processing*, 20(4):1286 – 1307, 2010.
17. Chin-Chen Chang and Pei-Yu Lin. Adaptive watermark mechanism for rightful ownership protection. *Journal of Systems and Software*, 81(7):1118 – 1129, 2008.
18. Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, and Tong-Yee Lee. A high capacity 3d steganography algorithm. *IEEE Transactions on Visualization and Computer Graphics*, 15(2):274–284, MAR-APR 2009.
19. Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3):727 – 752, 2010.
20. Rama Chellappa, Pawan Sinha, and P. Jonathon Phillips. Face recognition by computers and humans. *IEEE Computer*, 43(2):46–55, 2010.
21. Jiansheng Chen, Yiu-Sang Moon, Ming-Fai Wong, and Guangda Su. Palmprint authentication using a symbolic representation of images. *Image and Vision Computing*, 28(3):343 – 351, 2010.
22. Wei-Che Chen and Ming-Shi Wang. A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. *Expert Systems With Applications*, 36(2):1300–1307, MAR 2009.

23. R. J. Cintra, V. S. Dimitrov, H. M. de Oliveira, and R. M. Campello de Souza. Fragile watermarking using finite field trigonometrical transforms. *Signal Processing-Image Communication*, 24(7):587–597, AUG 2009.
24. I.J. Cox, M.L. Miller, and J.A. Bloom. Watermarking applications and their properties. In *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on*, pages 6 –10, 2000.
25. Ashraf Darwish and Ajith Abraham. The use of computational intelligence in digital watermarking: Review, challenges, and new trends. *Neural Network World*, 21(4):277–297, 2011.
26. Cheng Deng, Xinbo Gao, Xuelong Li, and Dacheng Tao. A local tchebichef moments-based robust image watermarking. *Signal Processing*, 89(8):1531–1539, AUG 2009.
27. Boris Efraty, Emil Bilgazyev, Shishir Shah, and Ioannis A. Kakadiaris. Profile-based 3d-aided face recognition. *Pattern Recognition*, 45(1):43 – 53, 2012.
28. Esam Elsheh and A. Ben Hamza. Secret sharing approaches for 3d object encryption. *Expert Systems with Applications*, 38(11):13906 – 13911, 2011.
29. Jie Gui, Wei Jia, Ling Zhu, Shu-Ling Wang, and De-Shuang Huang. Locality preserving discriminant projections for face and palmprint recognition. *Neurocomputing*, 73(13-15):2696 – 2707, 2010.
30. Won gyum Kim and HeungKyu Lee. Multimodal biometric image watermarking using two-stage integrity verification. *Signal Processing*, 89(12):2385 – 2399, 2009.
31. Madasu Hanmandlu, Jyotsana Grover, Ankit Gureja, and H.M. Gupta. Score level fusion of multimodal biometrics using triangular norms. *Pattern Recognition Letters*, 32(14):1843 – 1850, 2011.
32. Zhaofeng He, Tieniu Tan, Zhenan Sun, and Xianchao Qiu. Toward accurate and fast iris segmentation for iris biometrics. *IEEE Transactions On Pattern Analysis and Machine Intelligence*, 31(9):1670–1684, SEP 2009.
33. Karen Hollingsworth, Kevin W. Bowyer, and Patrick J. Flynn. Pupil dilation degrades iris biometric performance. *Computer Vision and Image Understanding*, 113(1):150 – 157, 2009.
34. Karen Hollingsworth, Kevin W. Bowyer, and Patrick J. Flynn. Useful features for human verification in near-infrared periocular images. *Image and Vision Computing*, 10.1016/j.imavis.2011.09.002(0):–, 2011.
35. Karen Hollingsworth, Kevin W. Bowyer, Stephen Lagree, Samuel P. Fenker, and Patrick J. Flynn. Genetically identical irises have texture similarity that is not detected by iris biometrics. *Computer Vision and Image Understanding*, 115(11):1493 – 1502, 2011.
36. Hone-Ene and Hwang. An optical image cryptosystem based on hartley transform in the fresnel transform domain. *Optics Communications*, 284(13):3243 – 3247, 2011.
37. Hsiang-Cheh Huang, Chi-Ming Chu, and Jeng-Shyang Pan. The optimized copyright protection system with genetic watermarking. *Soft Computing*, 13(4):333–343, FEB 2009. 2nd IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, CA, 2006.
38. A.K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):4 – 20, jan. 2004.
39. Jun Jin and Zhi hong Wu. A secret image sharing based on neighborhood configurations of 2-d cellular automata. *Optics & Laser Technology*, 10.1016/j.optlastec.2011.08.023(0):–, 2011.

40. Jongweon Kim, Namgyu Kim, Dongwon Lee, Sungbum Park, and Sangwon Lee. Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents. *Signal Processing-Image Communication*, 25(8):559–576, SEP 2010.
41. Kyung-Su Kim, Min-Jeong Lee, Hae-Yeoun Lee, and Heung-Kyu Lee. Reversible data hiding exploiting spatial correlation between sub-sampled images. *Pattern Recognition*, 42(11):3083–3096, NOV 2009.
42. Adams Kong, David Zhang, and Mohamed Kamel. A survey of palmprint recognition. *Pattern Recognition*, 42(7):1408–1418, JUL 2009.
43. Ajay Kumar and Arun Passi. Comparison and combination of iris matchers for reliable personal authentication. *Pattern Recognition*, 43(3):1016 – 1026, 2010.
44. Hyobin Lee, Jaehyuck Lim, Sunjin Yu, Sangki Kim, and Sangyoun Lee. Biometric image authentication using watermarking. In *SICE-ICASE, 2006. International Joint Conference*, pages 3950 –3953, oct. 2006.
45. Phen-Lan Lin, Yan-Hao Lai, and Po-Whei Huang. Dental biometrics: Human identification based on teeth and dental works in bitewing radiographs. *Pattern Recognition*, 45(3):934 – 946, 2012.
46. Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei, and Hualou Liang. A blind source separation-based method for multiple images encryption. *Image and Vision Computing*, 26(6):788 – 798, 2008.
47. Babak Mahdian and Stanislav Saic. A bibliography on blind methods for identifying image forgery. *Signal Processing-Image Communication*, 25(6):389–399, JUL 2010.
48. Gian Luca Marcialis, Fabio Roli, and Luca Didaci. Personal identity verification by serial fusion of fingerprint and face matchers. *Pattern Recognition*, 42(11):2807 – 2817, 2009.
49. Gian Luca Marcialis, Fabio Roli, and Daniele Muntoni. Group-specific face verification using soft biometrics. *Journal of Visual Languages & Computing*, 20(2):101 – 109, 2009.
50. Ilhem Benkara Mostefa, Sofiane Braci, Claude Delpha, Remy Boyer, and Mohammed Khamadja. Quantized based image watermarking in an independent domain. *Signal Processing-Image Communication*, 26(3):194–204, MAR 2011.
51. Nicolae and Duta. A survey of biometric technology based on hand shape. *Pattern Recognition*, 42(11):2797 – 2806, 2009.
52. Zhihong Pan, G. Healey, M. Prasad, and B. Tromberg. Face recognition in hyperspectral images. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(12):1552 – 1560, dec. 2003.
53. Miao Qi, Yinghua Lu, Ning Du, Yinan Zhang, Chengxi Wang, and Jun Kong. A novel image hiding approach based on correlation analysis for secure multimodal biometrics. *Journal of Network and Computer Applications*, 33(3):247 – 257, 2010.
54. Lishan Qiao, Songcan Chen, and Xiaoyang Tan. Sparsity preserving projections with applications to face recognition. *Pattern Recognition*, 43(1):331–341, JAN 2010.
55. R. Raghavendra, Bernadette Dorizzi, Ashok Rao, and G. Hemantha Kumar. Designing efficient fusion schemes for multimodal biometric systems using face and palmprint. *Pattern Recognition*, 44(5):1076 – 1088, 2011.
56. Venkatesh Ramanathan and Harry Wechsler. Robust human authentication using appearance and holistic anthropometric features. *Pattern Recognition Letters*, 31(15):2425 – 2435, 2010.
57. Gil Santos and Edmundo Hoyle. A fusion approach to unconstrained iris recognition. *Pattern Recognition Letters*, 10.1016/j.patrec.2011.08.017(0):–, 2011.

58. Ben Schouten and Bart Jacobs. Biometrics and their use in e-passports. *Image and Vision Computing*, 27(3):305–312, FEB 2 2009.
59. Caifeng Shan, Shaogang Gong, and Peter W. McOwan. Facial expression recognition based on local binary patterns: A comprehensive study. *Image and Vision Computing*, 27(6):803–816, MAY 4 2009.
60. Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang. Reversible data hiding based on histogram modification of pixel differences. *IEEE Transactions On Circuits and Systems for Video Technology*, 19(6):904–908, JUN 2009.
61. Alain Tremeau and Damien Muselet. Recent trends in color image watermarking. *Journal Of Imaging And Science Technology*, 53(1):010201, 2009.
62. Han-Min Tsai and Long-Wen Chang. Secure reversible visible image watermarking with authentication. *Signal Processing-Image Communication*, 25(1):10–17, JAN 2010.
63. Hsien-Wen Tseng and Chi-Pin Hsieh. Prediction-based reversible data hiding. *Information Sciences*, 179(14):2460–2469, JUN 27 2009.
64. Mustafa Ulutas, Guzin Ulutas, and Vasif V. Nabiyev. Medical image security and epr hiding using shamir's secret sharing scheme. *Journal of Systems and Software*, 84(3):341 – 353, 2011.
65. Mayank Vatsa, Richa Singh, and Afzel Noore. Feature based rdwt watermarking for multimodal biometric system. *Image and Vision Computing*, 27(3):293–304, FEB 2 2009.
66. Minghua Wan, Zhihui Lai, Jie Shao, and Zhong Jin. Two-dimensional local graph embedding discriminant analysis (2dlgeda) with its application to face and palm biometrics. *Neurocomputing*, 73(1-3):197 – 203, 2009.
67. Kai Wang, G. Lavoue, F. Denis, and A. Baskurt. A comprehensive survey on three-dimensional mesh watermarking. *Multimedia, IEEE Transactions on*, 10(8):1513 –1527, dec. 2008.
68. John Wright, Allen Y. Yang, Arvind Ganesh, S. Shankar Sastry, and Yi Ma. Robust face recognition via sparse representation. *IEEE Transactions On Pattern Analysis and Machine Intelligence*, 31(2):210–227, FEB 2009.
69. Chia-Chun Wu, Shang-Juh Kao, and Min-Shiang Hwang. A high quality image sharing with steganography and adaptive authentication scheme. *Journal of Systems and Software*, 84(12):2196 – 2207, 2011.
70. Dawen Xu, Rangding Wang, and Jicheng Wang. A novel watermarking scheme for h.264/avc video authentication. *Signal Processing-Image Communication*, 26(6):267–279, JUL 2011.
71. Yong Xu, David Zhang, and Jing-Yu Yang. A feature extraction method for use with bimodal biometrics. *Pattern Recognition*, 43(3):1106 – 1115, 2010.
72. Yong Xu, Qi Zhu, and David Zhang. Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments. *Neurocomputing*, 74(18):3946 – 3952, 2011.
73. Ching-Nung Yang and Tse-Shih Chen. Colored visual cryptography scheme based on additive color mixing. *Pattern Recognition*, 41(10):3114–3129, OCT 2008.
74. Ching-Nung Yang and Chuei-Bang Ciou. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image and Vision Computing*, 28(12):1600 – 1610, 2010.
75. Taiping Zhang, Bin Fang, Yuan Yuan, Yuan Yan Tang, Zhaowei Shang, Donghui Li, and Fangnian Lang. Multiscale facial structure representation for face recognition under varying illumination. *Pattern Recognition*, 42(2):251–258, FEB 2009.
76. Xinpeng Zhang and Shuozhong Wang. Fragile watermarking scheme using a hierarchical mechanism. *Signal Processing*, 89(4):675–679, APR 2009.

77. Hong Zhao, Hongxia Wang, and Muhammad Khurram Khan. Steganalysis for palette-based images using generalized difference image and color correlogram. *Signal Processing*, 91(11):2595 – 2605, 2011.
78. Zhi Zhong, Jie Chang, Mingguang Shan, and Bengong Hao. Fractional fourier-domain random encoding and pixel scrambling technique for double image encryption. *Optics Communications*, 285(1):18–23, 2012.
79. Nanrun Zhou, Yixian Wang, and Jianhua Wu. Image encryption algorithm based on the multi-order discrete fractional mellin transform. *Optics Communications*, 284(24):5588 – 5597, 2011.