Infrared Imagery and Border Control Systems

George Kumi Kyeremeh[1], Mohamed Abdul-Al[2], Rami Qahwaji[3] and Raed Abd-Alhameed[4]
{g.k.kyeremeh@bradford.ac.uk[1], m.abdul.al@bradford.ac.uk[2], r.s.r.qahwaji@bradford.ac.uk[3]; r.a.a.abd@bradford.ac.uk[4]}

Faculty of Engineering and Informatics, University of Bradford[1], Bradford, BD7 1DP, UK[1,2,3,4]

Abstract. The growing need for passenger authorization at international border crossing points (BCPs) is prompted research into more effective methods. Automated border control (ABC) is gaining attention in its ability to improve traveller ease, BCP throughput, and national security. Individuals are automatically recognized using a feature vector generated from their behavioural and/or physiological characteristics in biometric recognition. Biometric identification systems have been able to offer reliable personal recognition methods useful to validate or identify an individual. Visible spectrum images have some porosity and the effort to deal with it resulted in the introduction of Infrared imaging. This article is looked at verification and identification as the major components of a biometric system and the need for a multimodal system over a unimodal system of identification. It explained how infrared imaging support identification and verification and addresses some shortcomings of the visible spectrum with a comparison of the advantages and disadvantages of both media. Some limitations of Infrared imaging were also identified with multi-modal combining algorithms. The ethical issue to be observed in biometric identification are also discussed and the whole work concluded.

Keywords: Automated border control (ABC), Biometrics, Borders, e-Gate, electronic machine-readable travel document (e-MRTD), unimodal and multimodal, Infrared (IR), Visible spectrum.

1 Introduction

Biometric is derived from Greek words bios (life) and metrikos (measurement). Traditional recognition methods rely on what a person knows, such as a password, biometric recognition systems depend on who a person is, what they do, or how they respond to certain external stimuli. Biometrics offers several inherent advantages over conventional methodologies, biometric technology has developed as an enabling solution to automatically recognize people at a faster rate [1].

Border management broadly covers the concept of security and functionality. The security concept comes to play as borders are the primary line of defence for a sovereign country or nation. Border management implies a balance between these two concepts. The close borders will harm the economy and safety of any country while open borders will create security insufficiency. Establishing a sense of balance between enabling the flow of goods and persons across borders and delivering security procedures triggers the need for a Border Management Model. [2], [3]. A biometric system is a recognition system that identifies an individual based on an element vector derived through a characteristic of the behaviour or physiology. It can also

IMDC-IST 2021, September 07-09, Sakarya, Turkey

DOI 10.4108/eai.7-9-2021.2314979

be simply referred to as a pattern of recognition technology that works by collecting biometric data from a person, extracting a feature set from that data, and comparing that feature set to the system's registered template set. A biometric system can function in either verification or identification mode, depending on the application environment After useful data being extracted, the feature vector is usually saved in a database or on a smart device for the person. It may be easier to incorporate these data into a specific application, a biometric system dependent on physiological parameters is often more dependable than one based on behavioural variables [4], [5]. Passive sensors collect the infrared radiations generated by Thermal Imaging systems for any objects with temperatures above absolute zero. This technique of detection was originally developed for military surveillance and night vision devices, but it is now more economically viable, allowing for a wider range of applications than ever before.[6]. Most biometric systems rely on ordinary video cameras to record facial images in the visual spectrum. However, there is a growing need for infrared cameras due to an increased desire for a better security system and better monitoring in dark and poorly illuminated regions. The heat generated by the surveillance subject is captured by the thermal infrared camera, which creates a thermogram image utilising infrared radiation. These pictures are utilised in surveillance systems for object detection, identification, and the capacity to characterise observed things in detail. Because the camera can record faces from a distance, it is a non-intrusive method of identifying a person. People's identification or verification based just on thermal information may not be adequate for identification, but it might help a lot. [7], [8]. Biometrics has helped solve questions asked on daily basis such as:

1. Is this the right person to be allowed access to?
2. Does this person belong to this country?
3. Is this the authorized person for such action?

2 Biometric Systems

Four fundamental components make up a typical biometric system:

1. The biometric data is collected via a sensor module.
2. Feature vectors are extracted by processing the collected data in the feature extraction module.
3. Feature vectors are matched to the template in the matching module.
4. The user's identification is established and approved or denied in this decision-making module [5].

Biometric systems work in two different methods: verification and identification. The obtained biometric data is compared to templates corresponding to the claimed identity in verification, whereas the collected biometric data is compared to templates belonging to all users in the database in identification. As a result, identification and verification are two independent tasks that should be addressed individually as indicated in Fig. 1.

Verification: The system verifies the identity of a person in the verification mode by comparing recorded biometric data to the biometric template stored in the system database. The goal of identity verification is to prevent several persons from utilizing the same identity [9].

Identification: With identification, the system looks for a match in all the users' templates in the database to identify the individual. As a result, the system does a comparison of one too many to determine an individual's identification without requiring the subject to claim an identity; for example, "Whose biometric data is this?"). Negative recognition applications rely on identification to determine whether the person is who she claims to be (implicitly or explicitly). Negative recognition's goal is to stop a single individual from assuming many identities. For the sake of convenience, identification can also be employed in positive recognition. While traditional means of personal identification such as PINs and passwords, may work for identification, biometric is the sole way to establish negative identification [9].

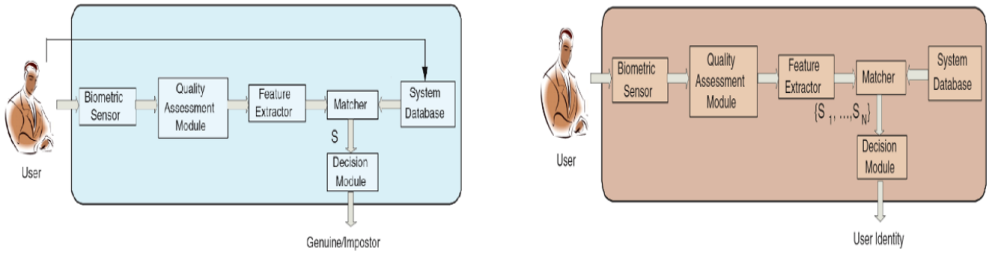

Fig 1. A block diagram of the tasks for verification and identification.[10].

2.1 Unimodal Biometric Systems

The limits of biometric systems that operate on a single biometric feature are as follows:

1. **Presence of noise in sensed data:** Data collected might be noisy or inaccurate. Defective or poorly maintained sensors or unfavourable ambient circumstances such as low lighting in a face recognition system can also cause noisy data. Biometric data that is noisy may be mismatched with database templates, resulting in an erroneous rejection of a user.
2. **Intra-class variations:** The authentication of an individual biometric data obtained may differ significantly from the data used to build the template during enrolment, causing the matching process to fail. During the verification phase, this variance is generally produced by a user who interacts with the sensor inappropriately or when sensor properties are changed.
3. **Distinctiveness:** Biometric characteristic is anticipated to vary considerably among people with the feature sets employed to describe these qualities may have a considerable inter-class similarity. The biometric trait's discriminability is limited because of these restrictions and as a result, every biometric characteristic has a theoretical upper constraint on its capacity to discriminate.
4. **Nonuniversality:** While every user is supposed to have the biometric feature that is being obtained, it is possible that a subset of users will not have that biometric. Due to the low quality of the ridges, a fingerprint biometric might unable to extract

characteristics from the fingerprints of specific individuals. As a result, utilizing a single biometric characteristic is associated with a failure to enrol (FTE) rate. According to estimates, up to 4% of the population may have low-quality fingerprint ridges that resulting in FTE mistakes.

5. **Spoofing attack:** To circumvent the system, an imposter could try to impersonate a valid registered user's biometric characteristic. When behavioural features like signature and voice are employed, spoofing attacks becomes much more significant whiles physical characteristics, on the other hand, are vulnerable to spoofing as well when used in a unimodal biometric system [11], [12, 13],[4].

2.2 Multimodal Biometric Systems

The use of many biometric modalities helps to overcome some of the limitations of unimodal biometric systems. These systems, known as multimodal biometric systems, are thought to be more trustworthy due to the availability of several, independent pieces of evidence. [10]. Multimodal biometric systems use more than one physiological or behavioural feature for enrolment, verification, or identification. Because the amount of data accessible for recognition has increased, these systems may be able to perform more reliable identity verifications. [14]. Face-based identity verification may not be effective in combatting identity theft unless multimodality is implemented. Improved matching performance would also result in a better user experience and an increase in passenger flow efficiency. The multimodal approach to identity verification is gaining traction in ABC systems, as seen by the growing number of deployments that have begun to use this technology [15]. Multimodal systems, on the other hand, have higher costs, acquisition times, and computational durations than typical monomodal systems and users may perceive a greater invasion of their privacy [16]. The multimodal biometric systems can be used under five conditions which as indicated in Fig. 2 is as follows:

1. Multiple sensors: information collected from multiple sensors for the same biometric is merged. Sensors based on optical and ultrasonic, for example, are available to obtain fingerprints.
2. Multiple biometrics: multiple biometric features are integrated, such as fingerprints and faces. These systems will very certainly have many sensors, each of which will detect a distinct biometric feature. Multiple biometrics are generally employed in a verification system to increase system accuracy, but a suitable combination scheme may also improve matching speed in an identity system.
3. Multiple units of the same biometric: Two or more fingerprints of a person's fingers may be combined, or one image from each of a person's two irises may be merged.
4. Multiple snapshots of the same biometric: for enrolment and/or recognition, more than one instance of the same biometric is utilised. Numerous imprints of the same finger, multiple voice samples, or multiple pictures of the face, for example, maybe merged.
5. Multiple matching and representations algorithms for the same biometric entails integrating diverse techniques and matching of the biometric trait after the feature has been extracted. There are two scenarios in which this may be useful. To begin, such a combination method can be used to create a recognition choice by a verification or identification. Second, such a combination technique for indexing may be used by an identifying system [11].

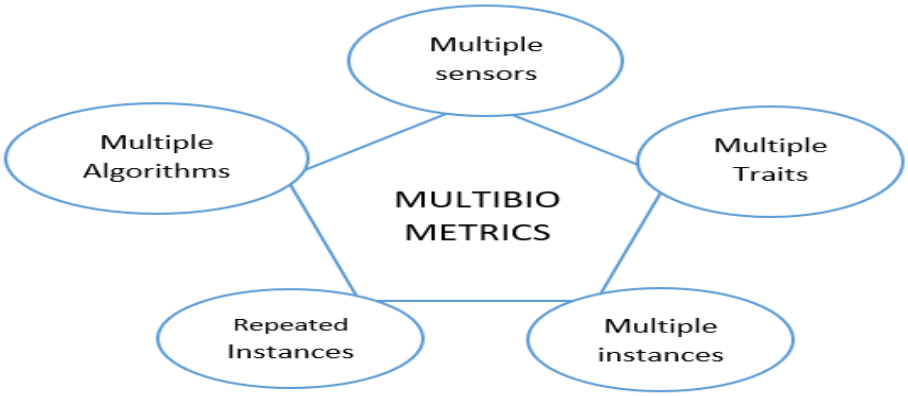

Fig 2. Five conditions under which multimodal biometric systems can be used [11].

3 Infrared (IR) System

Infrared radiation is the electromagnetic radiation that is released corresponding to the amount of heat created or reflected by an object, hence infrared imaging is also known as thermal imaging. The imaging wavelengths of visible light are shorter than infrared and renders invisible to the human eye. Infrared thermal sensors capture objects based on infrared light reflection or emitted infrared radiation [17]. The human face possesses a biometric characteristic that may be used to identify or authenticate people in security systems. Face recognition systems' major problem is properly matching the input face with a face image of the same person previously recorded in the system database. Face thermograms are used in the case of thermal face identification. The detection of a face in a picture is a related job and a requirement for facial recognition. A thermal face image should possess biometrics features that emphasize thermal face characteristics and are compact and straightforward to use for classification for thermal face identification [8]. It is important to identify characteristics that might be utilized in thermal biometrics since thermal face photographs give different information than visible spectrum images.

The study by [18],[19] considered face recognition under different environments intra-spectral and cross-spectral problems. They executed a test on different infrared bans against visible face images to evaluate the performance. They also verified under different environmental conditions and distances the different bands of infrared. An accuracy of 100 percent was obtained with visible image versus the (SWIR) of the IR band. This was done under a controlled environmental condition with a 30-meter distance.

Data collected with infrared cameras offer significant benefits than data collected with visible-spectrum cameras for face identification [20]. Thermal infrared images of the face may be produced in any lighting situation, even full darkness, and there is some indication that thermal infrared is more resistant to changes in facial expression [21]. Thermal infrared radiation is also less influenced by smoke or dust dispersion and absorption than visible light. In contrast to visible spectrum, infrared may extract not only external but also vital internal anatomical data, such as a face's vascular system [22], [23].

3.1. Limitations to Infrared Imaging

Using infrared images for automated facial identification comes with its own set of difficulties. In healthy persons, the human facial temperature is uniform and varies between 35.5°C and 37.5°C, producing a constant unique thermal signature to everyone.

1. The main disadvantage of thermal sub-band images in automatic face recognition is that several influencing factors affect the pattern of heat emitted the face is emitting, including postprandial metabolism, airflow, exercise, and ambient temperature. Regarding images by MWIR and LWIR, there is an aspect of sensitivity to external temperature, the subject's emotional, alcohol use, physical, as well as health state [24], [25].
2. The opaqueness of eyeglasses to most of the IR spectrum might be a concern (LWIR, MWIR, and SWIR). This implies that if a subject wears eyeglass, a substantial section of the face may be blocked, resulting in the loss of critical discriminative information [26], [27].
3. Another point of interest is the effect of sunshine on recognition if it is done outside and throughout the day. Although infrared sub-bands in the NIR and SWIR is unaffected by changes in visible light illumination, the appearance of infrared in the NIR and SWIR sub-bands is influenced by sunshine, which contains large spectral components [28], [26].
4. A survey by [62] exposed a series of shortcomings with which inhibited the further exploitation of infrared imaging, and they included the significant costs for thermal sensors, low resolution and excessive noise levels in pictures, the absence of publicly accessible infrared image data sets with the few available ones indicated in Table 1.

The mentioned shortcomings have predictably, led to and encouraged a new direction of study. Research by [29] suggested combining information from IR and visible ways to resolve the difficulty caused by opaque lenses. In combination with optical recording in infrared thermal imaging to alleviate the influence of emotional and health conditions on thermal images. Comparative thermal and optical images were analysed and able to record both optical and thermal images using charged coupled device (CCD) and low wave infrared (LWIR) microbolometer.

Table 1. Show a summary of main facial databases acquired in the infrared spectrum (Ghiass et al., 2014). The existence of variability data is signified by (●), limitation of variability signified by (ɵ), and very little to no variability by ○().

NAME	Primary Source	Used In	Subjects	Variability			
				Illumination	Pose	Expression	Time-Lapse
Equinox	[30]	[31],[32], [33], [34],[35], [36],[37], [38], [39], [39], e.t.c	90	●	○	●	○

IRIS thermal/Infrared	[40]	[41], [42],[43], [44]	32	●	●	●	○
IRIS-M3	[45]	[46], [45], [47], [48]	82	●	○	○	
University of Notre Dame	[49]	[50], [51],	241	ɵ	○	ɵ	●
University of Houston	[52]	[22],[53], [52],[54], [55]	138	○	●	●	○
Surveillance Camera Face Database	[56]		130	●	●	ɵ	ɵ
Florida State University	[57]	[57], [33]	10	○	●	●	○
UC Irvine hyperspectral	[58]	[58], [59], [60]	200	○	●	ɵ	●
West Virginia University Multispectral	[61]	[61], [62], [63]	50	○	●	○	ɵ
The Hong Kong Polytechnic University	[64]	[65]	335	○	ɵ	●	○
Laval University	[66]		200	○	●	●	●

Table 2. Recognition technique comparison for Thermal and Visual Imaging. (Kong et al., 2005)

Imaging methods	Advantages	Disadvantages
Visual Imaging	❖ Well-developed algorithms for recognition. ❖ The extraction and location of facial features are easier. ❖ Performs great when illumination conditions are controlled. ❖ Equipment (cameras) are less costly	❖ Facial expressions and illumination variation will lead to poor performance. ❖ In a cluttered scene, segmenting the face is difficult. ❖ Not useful under low lighting conditions. ❖ Difficult to detect disguise.
Thermal imaging	❖ Easy to segmentation, locate and detect faces. ❖ Smaller interclass variation. ❖ Not affected by illumination and facial expression. ❖ Great at detecting disguise.	❖ Thermal images are obstructed by the glass. ❖ Not suitable for objects/persons moving under speed. ❖ Thermal images have low image resolutions. ❖ Thermal equipment is expensive. ❖ Calibration will be required as environmental temperatures and activities can change the calibration.

Visual/Thermal Imaging	❖ Recognition accuracy is highly improved. ❖ Very broad areas of application ❖ Combined benefits of both cameras/sensors ❖ Detailed information of the anatomical and facial information of the face for better identification.	❖ Computational requirements are high. ❖ The complicated process of image setup. ❖ Thermal and Visual images require co-registration for data fusion

4 Ethical, Societal, And Legal Issues

Biometrics technology is widely recognized to pose significant ethical, societal, and legal issues. Ethical challenges are conditions in which a person must choose between two options that must be mediated as ethical or unethical. Social difficulties are issues that arise from regular social activities and have the potential to affect a significant number of people in a community. Legal challenges are official inquiries into the legality of the action and whether it is being carried out in conformity with the law.

Table 3. Values and the related vulnerabilities, risks, and mitigation measures [2].

VALUE	VULNERABILITY	RISK	POTENTIAL MITIGATION MEASURE
Right to no discrimination	Existing systems may be classified based on sex, race, ethnicity, or socioeconomic background, genetic characteristics, religion or belief, political stance, handicap, age, or sexual orientation, among other factors.	Individual sorting, social inclusion or exclusion, intolerance, and social inclusion or exclusion.	Biometrics for border control following human rights legislation must guarantee a non-discrimination policy.
Right to no information tracking	Current methods lack notifications and information regarding individual tracking.	Individuals and/or family members are subjected to monitoring because of violations of personal rights and legitimate purpose requirements.	Surveillance should be permitted and compliant with EU and national legislation if it serves a legitimate purpose.
Right to personal data protection	Personal data may slip into the wrong hands or be transferred between businesses under current methods.	Right to security principles such as confidentiality, integrity, and availability are violated.	Border control biometrics must provide Security by Design in order to preserve the continued confidentiality, availability, resilience, and integrity of processing systems and services.
Right to privacy and confidentiality	Modern systems may compromise the confidentiality, giving unauthorized access to sensitive data.	Violation of personal privacy.	Biometrics for border control must ensure the use of confidentiality enhanced technology to

			secure data in compliance with the law.
Concerning human dignity	Current solutions do not let individuals decide on the biometrics to enrol or utilize.	Right to human dignity, as well as cultural-religious practices, are violated	Unless choice is inapplicable, biometrics ay border control should give data explaining why biometrics are employed, as well as al-low choice rules and procedures.

5 Conclusion

Biometrics technology used in border control in two different perspectives has been presented. The primary objective of biometrics technology is to enhance management at border controls and increase the flow of people while considering ethical, legal, and social considerations have been considered. It was observed that Multimodal biometric systems are expected to have a lot of potential for future enhancement since they resolve issues posed by the unimodal biometric systems of recognition. Multimodal biometric systems may combine data at several levels, with fusion at the matching score level being the most common. They also solve the issues of non-universality and spoofing as well as increasing matching performance. Infrared imaging with IR thermal sensors can extend the life of lighting changes and work in low-light conditions. Additional physiological and anatomical face-related data, such as blood vessel structure and the thermal facial signature, may be collected via IR images and used by individuals as unique biometrics. Thermal face accuracy is fairly good, but there is still room for improvement. High accuracy is critical for security systems, since even the tiniest error might compromise national security and access control. The use of multi-modal combining methods by comparing thermal and optical pictures has emerged as a viable solution to curb any irregularities in the IR imaging system, and has been improved by employing a single charged coupled device (CCD) and low wave infrared (LWIR) microbolometer simultaneously.

Acknowledgments

This project has received funding from the European Union's Horizon-MSCA-RISE-2019-2023, Marie Skłodowska-Curie, Research and Innovation Staff Exchange (RISE), titled: Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control.

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to biometrics*. Springer Science & Business Media, 2011.

[2] M. Abomhara, S. Y. Yayilgan, A. H. Nymoen, M. Shalaginova, Z. Székely, and O. Elezaj, "How to do it right: a framework for biometrics supported border control," in *International Conference on e-Democracy*, 2019: Springer, pp. 94-109.

[3] L. R. Carlos-Roca, I. H. Torres, and C. F. Tena, "Facial recognition application for border control," in *2018 International Joint Conference on Neural Networks (IJCNN)*, 2018: IEEE, pp. 1-7.

[4] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE security & privacy*, vol. 1, no. 2, pp. 33-42, 2003.

[5] K. Delac and M. Grgic, "A survey of biometric recognition methods," in *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*, 2004: IEEE, pp. 184-193.

[6] M. Rai, T. Maity, and R. Yadav, "Thermal imaging system and its real time applications: a survey," *Journal of Engineering Technology*, vol. 6, no. 2, pp. 290-303, 2017.

[7] D. O. Gorodnichy, E. Granger, and P. Radtke, "Survey of commercial technologies for face recognition in video," 2014.

[8] M. Kristo and M. Ivasic-Kos, "An overview of thermal face recognition methods," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018-05-01 2018: IEEE, doi: 10.23919/mipro.2018.8400200.

[9] J. L. Wayman, "Fundamentals of biometric authentication technologies," *International Journal of Image and Graphics*, vol. 1, no. 01, pp. 93-113, 2001.

[10] A. K. Jain, "Biometric recognition: overview and recent advances," in *Iberoamerican Congress on Pattern Recognition*, 2007: Springer, pp. 13-19.

[11] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4-20, 2004.

[12] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial" gummy" fingers on fingerprint systems," in *Optical Security and Counterfeit Deterrence Techniques IV*, 2002, vol. 4677: International Society for Optics and Photonics, pp. 275-289.

[13] A. Eriksson and P. Wretling, "How flexible is the human voice?-a case study of mimicry," in *Fifth European Conference on Speech Communication and Technology*, 1997.

[14] A. K. Jain and A. Ross, "Multibiometric systems," *Communications of the ACM*, vol. 47, no. 1, pp. 34-40, 2004.

[15] M. Kosmerlj, T. Fladsrud, E. Hjelmås, and E. Snekkenes, "Face recognition issues in a border control environment," in *International Conference on Biometrics*, 2006: Springer, pp. 33-39.

[16] A. Ross, K. Nandakumar, and A. Jain, "Handbook of Multibiometrics, ser. Int. Series on Biometrics. Secaucus," ed: NJ: Springer-Verlag, 2006.

[17] C. Solomon and T. Breckon, *Fundamentals of Digital Image Processing: A practical approach with examples in Matlab*. John Wiley & Sons, 2011.

[18] K. R. Kakkirala, S. R. Chalamala, and S. K. Jami, "Thermal infrared face recognition: A review," in *2017 UKSim-AMSS 19th International Conference on Computer Modelling & Simulation (UKSim)*, 2017: IEEE, pp. 55-60.

[19] T. Bourlai and B. Cukic, "Multi-spectral face recognition: Identification of people in difficult environments," in *2012 IEEE International Conference on Intelligence and Security Informatics*, 2012: IEEE, pp. 196-201.

[20] G. Friedrich and Y. Yeshurun, "Seeing people in the dark: Face recognition in infrared images," in *International Workshop on Biologically Motivated Computer Vision*, 2002: Springer, pp. 348-359.

[21] F. Nicolo and N. A. Schmid, "A method for robust multispectral face recognition," in *International Conference Image Analysis and Recognition*, 2011: Springer, pp. 180-190.

[22] P. Buddharaju, I. T. Pavlidis, and P. Tsiamyrtzis, "Physiology-based face recognition," in *IEEE Conference on Advanced Video and Signal Based Surveillance, 2005.*, 2005: IEEE, pp. 354-359.

[23] I. Pavlidis and P. Symosek, "The imaging issue in an automatic face/disguise detection system," in *Proceedings IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications (Cat. No. PR00640)*, 2000: IEEE, pp. 15-24.

[24] A. Matthews, "Ophthalmic antimicrobial therapy in the horse," *Equine Veterinary Education*, vol. 21, no. 5, pp. 271-280, 2009.

[25] F. J. Prokoski and R. B. Riedel, "Infrared identification of faces and body parts," in *Biometrics*: Springer, 1996, pp. 191-212.

[26] S. Z. Li, R. Chu, S. Liao, and L. Zhang, "Illumination invariant face recognition using near-infrared images," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 627-639, 2007.

[27] S.-Q. Wu *et al.*, "Infrared face recognition by using blood perfusion data," in *International Conference on Audio-and Video-Based Biometric Person Authentication*, 2005: Springer, pp. 320-328.

[28] S.-Q. Wu, L.-Z. Wei, Z.-J. Fang, R.-W. Li, and X.-Q. Ye, "Infrared face recognition based on blood perfusion and sub-block DCT in wavelet domain," in *2007 International Conference on Wavelet Analysis and Pattern Recognition*, 2007, vol. 3: IEEE, pp. 1252-1256.

[29] S. G. Kong, J. Heo, B. R. Abidi, J. Paik, and M. A. Abidi, "Recent advances in visual and infrared face recognition—a review," *Computer Vision and Image Understanding*, vol. 97, no. 1, pp. 103-135, 2005.

[30] D. Socolinsky, "Human Identification at a Distance Database," *Equinox Corp., USA*.

[31] D. A. Socolinsky and A. Selinger, "A comparative analysis of face recognition performance with visible and thermal infrared imagery," in *Object recognition supported by user interaction for service robots*, 2002, vol. 4: IEEE, pp. 217-222.

[32] D. A. Socolinsky, A. Selinger, and J. D. Neuheisel, "Face recognition with visible and thermal infrared imagery," *Computer vision and image understanding*, vol. 91, no. 1-2, pp. 72-114, 2003.

[33] A. Srivastava and X. Liu, "Statistical hypothesis pruning for identifying faces from infrared images," *Image and Vision Computing*, vol. 21, no. 7, pp. 651-661, 2003.

[34] A. Gyaourova, G. Bebis, and I. Pavlidis, "Fusion of infrared and visible images for face recognition," in *European Conference on Computer Vision*, 2004: Springer, pp. 456-468.

[35] J. Heo, S. G. Kong, B. R. Abidi, and M. A. Abidi, "Fusion of visual and thermal signatures with eyeglass removal for robust face recognition," in *2004 Conference on Computer Vision and Pattern Recognition Workshop*, 2004: IEEE, pp. 122-122.

[36] B. Abidi, S. Huq, and M. Abidi, "Fusion of visual, thermal, and range as a solution to illumination and pose restrictions in face recognition," in *38th Annual 2004 International Carnahan Conference on Security Technology, 2004.*, 2004: IEEE, pp. 325-330.

[37] P. Buddharaju, I. Pavlidis, and I. Kakadiaris, "Face recognition in the thermal infrared spectrum," in *2004 Conference on Computer Vision and Pattern Recognition Workshop*, 2004: IEEE, pp. 133-133.

[38] S. Singh, A. Gyaourova, G. Bebis, and I. Pavlidis, "Infrared and visible image fusion for face recognition," in *Biometric technology for human identification*, 2004, vol. 5404: International Society for Optics and Photonics, pp. 585-596.

[39] J. Heo, M. Savvides, and B. Vijayakumar, "Advanced correlation filters for face recognition using low-resolution visual and thermal imagery," in *International Conference Image Analysis and Recognition*, 2005: Springer, pp. 1089-1097.

[40] Y. M. Elbarawy, N. I. Ghali, and R. S. El-Sayed, "Facial expressions recognition in thermal images based on deep learning techniques," *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, vol. 11, no. 10, pp. 1-7, 2019.

[41] O.-K. Kwon and S. G. Kong, "Multiscale fusion of visual and thermal images for robust face recognition," in *CIHSPS 2005. Proceedings of the 2005 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2005.*, 2005: IEEE, pp. 112-116.

[42] M. K. Bhowmik, D. Bhattacharjee, M. Nasipuri, D. K. Basu, and M. Kundu, "Classification of polar-thermal eigenfaces using multilayer perceptron for human face recognition," in *2008 IEEE Region 10 and the Third international Conference on Industrial and Information Systems*, 2008: IEEE, pp. 1-6.

[43] M. K. Bhowmik, D. Bhattacharjee, M. Nasipuri, D. K. Basu, and M. Kundu, "Optimum fusion of visual and thermal face images for recognition," in *2010 Sixth International Conference on Information Assurance and Security*, 2010: IEEE, pp. 311-316.

[44] O. Arandjelović, R. Hammoud, and R. Cipolla, "Thermal and reflectance based personal identification methodology under variable illumination," *Pattern Recognition*, vol. 43, no. 5, pp. 1801-1813, 2010.

[45] H. Chang, H. Harishwaran, M. Yi, A. Koschan, B. Abidi, and M. Abidi, "An indoor and outdoor, multimodal, multispectral and multi-illuminant database for face recognition," in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, 2006: IEEE, pp. 54-54.

[46] H. Chang, A. Koschan, B. Abidi, and M. Abidi, "Physics-based fusion of multispectral data for improved face recognition," in *18th International Conference on Pattern Recognition (ICPR'06)*, 2006, vol. 3: IEEE, pp. 1083-1086.

[47] H. Chang, Y. Yao, A. Koschan, B. Abidi, and M. Abidi, "Spectral range selection for face recognition under various illuminations," in *2008 15th IEEE International Conference on Image Processing*, 2008: IEEE, pp. 2756-2759.

[48] H. Chang, Y. Yao, A. Koschan, B. Abidi, and M. Abidi, "Improving face recognition via narrowband spectral range selection using Jeffrey divergence," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, pp. 111-122, 2009.

[49] J. Doyle and K. Bowyer, "Notre Dame Image Database for Contact Lens Detection in Iris Recognition—2013," ed, 2014.

[50] X. Chen, P. J. Flynn, and K. W. Bowyer, "IR and visible light face recognition," *Computer Vision and Image Understanding*, vol. 99, no. 3, pp. 332-358, 2005.

[51] X. Chen, P. J. Flynn, and K. W. Bowyer, "PCA-based face recognition in infrared imagery: Baseline and comparative studies," in *2003 IEEE International SOI Conference. Proceedings (Cat. No. 03CH37443)*, 2003: IEEE, pp. 127-134.

[52] P. Buddharaju, I. T. Pavlidis, P. Tsiamyrtzis, and M. Bazakos, "Physiology-based face recognition in the thermal infrared spectrum," *IEEE transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 613-626, 2007.

[53] P. Buddharaju, I. T. Pavlidis, and P. Tsiamyrtzis, "Pose-invariant physiological face recognition in the thermal infrared spectrum," in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, 2006: IEEE, pp. 53-53.

[54] P. Buddharaju and I. Pavlidis, "Physiological face recognition is coming of age," in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009: IEEE, pp. 128-135.

[55] S.-Y. Cho, L. Wang, and W. J. Ong, "Thermal imprint feature analysis for face recognition," in *2009 IEEE International Symposium on Industrial Electronics*, 2009: IEEE, pp. 1875-1880.

[56] M. Grgic, K. Delac, and S. Grgic, "SCface–surveillance cameras face database," *Multimedia tools and applications*, vol. 51, no. 3, pp. 863-879, 2011.

[57] A. Srivastava, X. Liu, B. Thomasson, and C. Hesher, "Spectral probability models for infrared images and their applications to ir face recognition," in *º Proc. Workshop Computer Vision Beyond Visual Spectrum*, 2001.

[58] Z. Pan, G. Healey, M. Prasad, and B. Tromberg, "Face recognition in hyperspectral images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 12, pp. 1552-1560, 2003.

[59] Z. Pan, G. E. Healey, M. Prasad, and B. J. Tromberg, "Hyperspectral face recognition under variable outdoor illumination," in *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery X*, 2004, vol. 5425: International Society for Optics and Photonics, pp. 520-529.

[60] Z. Pan, G. E. Healey, and B. Tromberg, "Multiband and spectral eigenfaces for face recognition in hyperspectral images," in *Biometric Technology for Human Identification II*, 2005, vol. 5779: International Society for Optics and Photonics, pp. 144-151.

[61] T. Bourlai, N. Kalka, A. Ross, B. Cukic, and L. Hornak, "Cross-spectral face verification in the short wave infrared (SWIR) band," in *2010 20th International Conference on Pattern Recognition*, 2010: IEEE, pp. 1343-1347.

[62] T. Bourlai and Z. Jafri, "Eye detection in the middle-wave infrared spectrum: towards recognition in the dark," in *2011 IEEE International Workshop on Information Forensics and Security*, 2011: IEEE, pp. 1-6.

[63] N. D. Kalka, T. Bourlai, B. Cukic, and L. Hornak, "Cross-spectral face recognition in heterogeneous environments: A case study on matching visible to short-wave infrared imagery," in *2011 International Joint Conference on Biometrics (IJCB)*, 2011: IEEE, pp. 1-8.

[64] B. Zhang, L. Zhang, D. Zhang, and L. Shen, "Directional binary code with application to PolyU near-infrared face database," *Pattern Recognition Letters*, vol. 31, no. 14, pp. 2337-2344, 2010.

[65] L. Shen, J. He, S. Wu, and S. Zheng, "Face recognition from visible and near-infrared images using boosted directional binary code," in *International Conference on Intelligent Computing*, 2011: Springer, pp. 404-411.

[66] R. S. Ghiass, O. Arandjelović, H. Bendada, and X. Maldague, "Illumination-invariant face recognition from a single image across extreme pose using a dual dimension AAM ensemble in the thermal infrared spectrum," in *The 2013 International Joint Conference on Neural Networks (IJCNN)*, 2013: IEEE, pp. 1-10.