A SURVEY ON IMAGE SECURITY AND BIOMETRICS

Ms.P.Shobana 1 ,Research Scholar of Pollachi College of Arts and Science and Assistant Professor in Information Technology1, Sree Saraswathi Thyagaraja College Pollachi, Coimbatore, India, Shobana.send2@gmail.com

Dr.D.Kannan 2, Principal, Pollachi College of Arts and Science, Poosaripatti Post, Pollachi

Mr.P.Boopathi 3, Assistant Professor in Department of Computer Applications 3, Nehru Arts and Science College, Coimbatore

Mr.M.Mohan Kumar 4, Student, Department of Information Technology 4, Sree Saraswathi Thyagaraja College, Pollachi

ABSTRACT

Biometrics and image security are two fields that are strongly related. The necessity to protect biometric data has increased due to the speedy development of biometrics. Due to the visual nature of the majority of this data, image security techniques for biometric applications have undergone extensive development. In this study, we quickly review imaging-related biometrics and image security strategies. We offer the most recent research on how these two domains interact. The computational methods are the main focus of this research.

Keywords: Biometrics, Imaging Security, Watermarking, Image Cryptography, Steganography.

1 INTRODUCTION:

Data security is an important and growing area of IT. The first asset for security is text. Today's digital processes also use visual information. Recent years have seen a growing interest in image and data security techniques.

1. The authenticity and/or ownership of the image maker or sender may be the objectives.
2. The accuracy of the image data and the capability to detect image manipulation.
3. Data privacy, including ownership and/or content.

The techniques must typically compel additional aspects that might be required, such as performance requirements (speed, memory utilization, etc.), usability criteria (user-friendliness, low expertise needs, etc.), and other usable features. There have been some security methods used, including steganography and watermarking [1,82].

It has also been done to adapt classical cryptography to image data [2,3,4]. Due to the nature of the image data, research interest in the following areas has lately increased: The demand for secure biometrics storing and sharing systems is increasing more as biometric systems use image techniques. The relationship between these two locations is depicted in Figure 1. In section 2, this paper provides an overview of the cited image security research topics, highlighting the most recent advancements. The section 3 introduces image biometrics and describes how image security methods are being used in it. The section presents the final conclusions.

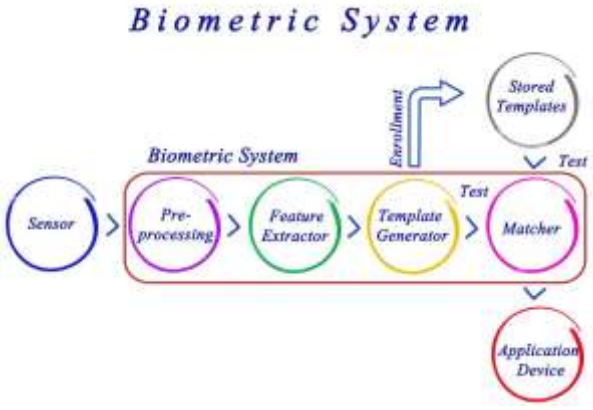

Fig. 1. A simple flowchart that illustrates the relation between biometrics system.

2 IMAGE SECURITIES:

Securing the storage and transmission of images is one of the cornerstones of information security. Communication protocols such as Secure Sockets Layer (SSL) use message Authentication codes to ensure the correct identities of the sender and receiver of data fragments on the Internet. Similarly, authentication, integrity and data hiding measures can also be applied to multimedia content such as audio, images or video. The two main approaches to authentication in imaging science are watermarking and cryptography.

The main difference between both methods is that the purpose of the watermark is to represent the owner's signature without changing the visual perception of the data. On the other hand, encrypted images cannot be read without decryption. Most watermarking methods and encryption systems also seek data integrity. Image steganography could be seen as a special case of watermarking, where the goal is to hide information in the image.

2.1 Watermarking

The purpose of a watermark is to insert information into an image by making changes that must meet three requirements:

1) To be invisible to the human eye,
2) To be recoverable by computer software, and
3) To be designed and built in such a way those attackers cannot access it.

These requirements and the nature of the image data lead to certain characteristics that watermarking algorithms must meet [5, 6].

Fidelity: The higher the fidelity, the harder it is to detect the watermark. This is not a computer property, but a subjective measure of visual perception.

Size: This property corresponds to the amount of data that the watermark can contain.

Robustness: The watermarking process must withstand passive distortion. These distortions can be caused by image processing, transmission and recording distortions. Resilience also corresponds to the ability of a watermark to resist attacks such as watermark removal, covert communication detection, covert attacks, or spoofing attacks. These features may conflict, so there must be an appropriate compromise between them in the watermarking process. Tremeau et al. gave a good example of these phenomena [5]. In order for the watermark to be stable, it should be placed in the most important parts of the information. In fact, many watermark attacks damage perceived less important components by compressing them. However, to maintain high accuracy, the perceptually less important parts of the data must be watermarked. Therefore solidity and loyalty are in conflict. To find the right balance between these functions, it is important to have a good understanding of the application area of the watermarking process. These applications include [6]

Ownership Verification: The owner of the image can create and insert a unique watermark. The user can make a watermark based on the private key. Not only can he verify his identity, but he can also claim ownership of the image because he is the only one who knows the key.

Data integrity: Any change made to the image will also affect the watermark.

Fingerprinting: Transactional watermarks allow linking 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 as a copy control system. Instead of preventing illegal copies, watermarking can track the illegal activity. Media players 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 studied [7], watermarks are invaluable tools for image forensics. Another important topic is copyright protection. Many algorithms are designed and tested for a specific video codec or image format [8]. Some applications, like medical imaging or arts storage require that the data cannot be modified -i.e. losses or lossy to-lossles procedures. Another aspect affecting the development of watermarks is what to encode, for example a 2-Dimensional bar code [9] or a logo [10]. There is also a growing interest in fusing watermark-protected biometric data [11]. Besides well-known two dimensional images and video watermarking, research on watermark insertion in three dimensional visual data has also been developed [12]. There has been wide interest in the use of computational intelligence methods for watermarking and are extensively revised in [13]. Some methods use signal processing approaches like wavelet transforms [14] and Independent Component Analysis [15]. In this line of work, other researchers propose fuzzy clustering approaches [16], genetic algorithms [17] or hybrid approaches [18,19]. 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 [20,21]. It is also interesting the ability of not only detecting unwanted modifications but also recovering the original image [22].

2.2 Image Cryptography:

Image encryption aims to hide its content from unauthorized viewers and authenticate its owner. Classic cryptography focused on text data [23]. Image Security and Biometrics: A review

439 Today, there is more research focusing on image data. The idea is to use visual information as different components that make up a cryptographic system. In

addition, it is desirable that the procedure does not require additional optical hardware [24]. For example, the amplitude distribution of the Hartley transform can be the public key and the phase distribution the private key [24]. Other similar approaches use Mellin transforms [25], Fractional Fourier transforms [26] or blind source separation algorithms [27]. Another cryptography applied to images is visual encryption. The idea is to divide the visual information into meaningless frames and share it between users. An image can only be reconstructed if all parts are somehow masked, hopefully without loss of information [2,3,4]. These methods do not require keys because the human visual system decrypts the data. Visual cryptography is closely related to Stenography, which is discussed below. 2.3.

2.3 Information Hiding on Images:

Steganography is the science of hiding and transmitting secret information using multimedia media such as images or videos. Its purpose is to hide the presence of confidential information. This is a key feature of applications dealing with secret data, such as medical image sharing [28]. Cheddad et al. [29] recently published an exhaustive survey of image steganography. We focus on computational intelligence tools and recent publications on the subject. Most algorithms work in the spatial [30, 31] or frequency [32] domain. They use computational tools such as predictors [33], particle swarm optimization [34] or fuzzy detectors [35].

Recently, adaptive algorithms being developed that use more information from the image [29, 36,37]. The Combining statistical and frequency data with knowledge of image objects or textures can yield better results [29]. Some of these approaches even try to improve image quality during data embedding [36]. These techniques, of course, depend on the image format and are generally not intended for palette-based images [37]. 3D models can also be steganography. Previous attempts to hide 3D models were usually modified watermarking techniques. Only since 2009 have researchers started designing 3D steganography algorithms. Chao et al. [38] proposed a multi layered method. It had high power, but was not immune to certain malicious attacks such as smoothing, addtional noise, uneven scaling, simplification, and verticies resampling. In 2010, Amat et al. developed a lossless algorithm where the positions of the peaks were not changed [39]. Their method is based on minimum spanning trees. Other recent studies are based on 2D imaging techniques [40].

3 BIOMETRICS AND IMAGE SECURITY:

The importance of image security is most notable in biometrics. Biometrics consists of a collection of methods to unambiguously identify an object (usually a 440 I. Marqués and M. Graña human, but it can also be other animal species). Biometric algorithms and methods must follow a system that verifies the subject's identity using biological properties: fingerprint, facial image, DNA sequence, voice, gait, etc. Many of these techniques are closely related to image science - see Table 1. Some methods aim to identify a single object, while others require authentication of a person [41]. Most biometric systems require strong security. Therefore, they usually use watermarking, cryptography and steganography.

3.1Three Types of Biometrics Security

Although they may have other applications, biometrics has often been used in security, and for the most part, biometrics can be classified into three groups:

1. Biological biometrics
2. Morphological biometrics
3. Behavioral biometrics

Biological biometrics uses characteristics at the genetic and molecular level. These may include characteristics such as DNA or blood, which can be assessed using a sample of body fluids. **Morphological biometrics** is about the structure of your body. More physical features such as eyes, fingerprints or facial shape can be mapped for use with security scanners.

Behavioral biometrics are based on models that are unique to each individual. How you walk, talk or even type on your keyboard can be an indicator of your identity if these patterns are tracked.

3.2Biometric Security Works

Biometric identification plays an increasing role in our everyday security. Physical characteristics are relatively fixed and individual - also in twins. Each unique biometric identity can be used to replace, or at least supplement, password systems for computers, telephones, and restricted access rooms and buildings. Once the biometric data is acquired and mapped, it is stored so that it can be compared against future access attempts. In most cases, this information is encrypted and stored on the device or on a remote server.[82]

Biometric scanners are devices used to collect biometric data for identity verification. These controls match the stored database to approve or deny access to the system. In other words, biometric security means that your body becomes the "key" to unlock access. Biometrics is widely used to achieve two main benefits:

Ease of use: Biometric data is always with you and cannot be lost or forgotten.

Difficult to steal or impersonate: Biometric data such as password or key cannot be stolen. While these systems aren't perfect, they hold a lot of promise for the future of cyber security.

3.3Examples of Biometric Security

Here are some common examples of biometric security:

- voice recognition
- Fingerprint scanning
- Facial recognition
- Iris recognition

- Heart rate sensor

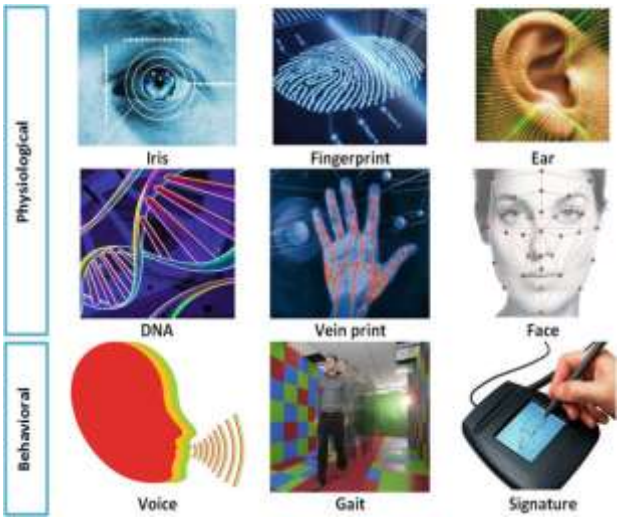

Fig. 3.1 Types of Biometric Security

Biometric scanners are becoming increasingly sophisticated. You can even find biometric data in your phone's security systems. For example, the facial recognition technology in Apple's iPhone X projects 30,000 infrared dots onto a user's face, authenticating the user through pattern matching. According to Apple, the risk of iPhone X biometrics being misidentified is one in a million. The LG V30 smart phone combines facial and voice recognition with fingerprint scanning and saves data on the phone for added security. Sensor maker Crucial Tec attaches pulse sensors to its fingerprint readers for two-step verification. This helps ensure that your systems cannot be accessed using the copy fingerprint. The challenge is that biometric scanners, including facial recognition systems, can be fooled. Researchers at the University of North Carolina at Chapel Hill downloaded photos of 20 volunteers from social media and used them to build 3D models of their faces. The researchers managed to break four of the five security systems they tested. Examples of fingerprint cloning abound. An example from the Black Hat cyber security conference showed that fingerprints can be reliably reproduced in about

0 minutes with $10 hardware, simply by making them on molded plastic or waxes. Germany's Chaos Computer Club spoofed the iPhone's TouchID fingerprint reader within two days of the iPhone's launch. The team simply took a fingerprint from the glass surface and used it to unlock the iPhone 5s.

In practice, biometric security has been proven in many areas. Advanced biometrics are used to protect sensitive documents and valuables. Citibank already uses voice recognition, and Halifax Bank in the UK is testing devices that monitor heartbeats to verify customers' identities. Ford is even considering installing biometric sensors in cars. Biometrics are being integrated into e-passports around the world. In the United States, electronic passports contain a chip that contains a digital image of your face, fingerprint, or iris, and technology that prevents the chip from being read and the data from being displayed to unauthorized data readers. We will see the pros and cons in real time as these security systems are deployed.

Fig. 3.2 Types of Biometrics Authentication

3.4 Biometric Scanners - Improvements and Concerns:

Biometric scanners are becoming increasingly sophisticated. You can even find biometric data in your phone's security systems. For example, the facial recognition technology in Apple's iPhone X projects 30,000 infrared dots onto a user's face, authenticating the user through pattern matching. According to Apple, the risk of iPhone X biometrics being misidentified is one in a million. The LG V30 smart phone combines facial and voice recognition with fingerprint scanning and saves data on the phone for added security. Sensor maker CrucialTec attaches pulse sensors to its fingerprint readers for two-step verification. This helps ensure that your systems cannot be accessed using the copy fingerprint. The challenge is that biometric scanners, including facial recognition systems, can be fooled. Researchers at the University of North Carolina at Chapel Hill downloaded photos of 20 volunteers from social media and used them to build 3D models of their faces. The researchers managed to break four of the five security systems they tested. Examples of fingerprint cloning abound. An example from the Black Hat cybersecurity conference showed that fingerprints can be reliably reproduced in about

0 minutes with $10 hardware, simply by making them on molded plastic or waxes. Germany's Chaos Computer Club spoofed the iPhone's TouchID fingerprint reader within two days of the iPhone's launch. The team simply

took a fingerprint from the glass surface and used it to unlock the iPhone 5s.

3.5 Biometrics - Identity & Privacy Concerns

Biometric authentication is convenient, but privacy advocates fear that biometric security will erodes privacy. The concern is how easy it is to collect personal data without consent. Facial recognition is part of daily life in Chinese cities, used in everyday shopping, and London is known to be full of CCTV cameras. Today, New York, Chicago and Moscow connect their cities' CCTV cameras to facial recognition databases to help local police fight crime. To advance the technology, Carnegie Mellon University is developing a camera that can scan the irises of people in a crowd at a distance of 10 meters. In 2018, facial recognition was introduced in Dubai airport, where travelers are photographed by 80 cameras as they pass through a tunnel in a virtual aquarium. Facial recognition cameras are also at work in other airports throughout the world, including those in Helsinki, Amsterdam, Minneapolis-St. Paul, and Tampa. All that data must be stored somewhere, fueling fears of constant surveillance and misuse of data…

Biometric Data Security Concerns

A more immediate problem is that databases of personal information are targets for hackers. For example, when the U.S. Office of Personnel Management was hacked in 2015, cybercriminals made off with the fingerprints of 5.6 million government employees, leaving them vulnerable to identity theft. Storing biometric data on a device – like the iPhone's TouchID or Face ID – is considered safer than storing it with a service provider, even when the data is encrypted. This risk is similar to password databases, where hackers can break into systems and effectively steal unlocked data. However, the results were completely different. If the password has been hacked, it can be changed. The biometric data remains fixed in the contract forever.

3.6 Ways to Protect Biometric Identity

Due to privacy and security risks, additional safeguards must be built into biometric systems. Unauthorized access is made more difficult when the system requires multiple authentication methods, such as life detection (such as flashing) and matching encrypted samples to users in encrypted domains. Some security systems also include additional features such as age, gender and height to thwart hackers' biometrics. The Aadhaar program of the Single Identity Authority of India is a good example. Launched in 2009, the multi-step authentication software combines iris scanning, ten fingerprints and facial recognition. This information is linked to the unique identity card issued to each of India's 1.2 billion citizens. Soon, the card will be mandatory for anyone using social services in India. Biometrics can be a good substitute for usernames as part of a two-factor authentication strategy.

That incorporates:

1. Something you have (biometrics)

2. Something you know (such as a password)

Two-factor authentication is a powerful combination, especially with the proliferation of IoT devices.

With additional safeguards, secure Internet-connected devices are less vulnerable to data breaches. Also, using a password manager to store traditional passwords can give you an extra layer of protection. By definition, a biometric system should have certain characteristics, among other considerations [42, 43]:

Universal: Applies to all humans.

Uniqueness: The biometrics of the two subjects must be sufficiently different. Persistence: Biometrics must be continuous over time. Obtaining or verifying it will not alter the user's biometrics.

Compilability: Features can be quantified.

Performance: Accuracy, speed, low resource consumption, and stability to environmental factors are desirable.

Acceptance: It is important to measure community acceptance of a particular biometric feature.

Security: Biometric systems must ensure authenticity, integrity, confidentiality and resistance to attack and falsification.

3.7 Imaging and Biometrics

Facial recognition [44] is one of the most relevant applications for image analysis. It has been widely proposed and used as a biometric. Indeed, building an automated system that matches human facial recognition capabilities is one of the major challenges in the field of biometrics. Facial recognition can be about authenticating users, which is a binary decision problem. This usually involves finding a subject's identity in a large database of faces, which is a (big) layered problem. This initial problem may extend to looking and expressing or recognizing emotions [45]. Recent studies on this topic have used classical approaches such as finding optimal discriminative projections that seek space preservation [46], supervised discriminative methods [47] or grid computing algorithms [48]. Another approach is not to select the best features, but to obtain a sufficient number of features using parsimony conservation methods [49, 50].

Frequency-based algorithms such as the wavelet transform have also been used [51]. Several studies have attempted to use stereoscopic geometric features, although this approach has received less attention recently. This approach is an example of so-called soft biometrics. This "simple" branch of biometrics is used to extract features (such as skin or eyes, or non-facial features such as ethnicity). Improving the "hard" biometric methods of face recognition can be beneficial [52]. Incidentally, the applicability of infrared or near-

infrared imaging for face recognition remains an open question [53], as the infrared signature of a face can change dramatically over time. However, infrared information can help facial recognition systems overcome differences in posture, illumination, and expression [54]. 3D information is also used to construct stable systems for these problems [55]. Unlike face recognition, iris scanners usually require the subject to move. In other words, the user must stand close to the iris scanner and remain still. One of the goals of iris biometry is to design less invasive collection procedures [56]. This is inconvenient for the user, but avoids problems like occlusion or looking for the wrong images. Another advantage is that the biometric system can distinguish the left eye from the right eye and the iris of identical twins [57]. On the other hand, iris biometrics has problems of deterioration caused by pupil dilation [58] or contact lenses [59]. Another problem is iris fragmentation. The iris recognition system must extract the iris area and remove the pupils, eyelids, sclera, etc. Recent studies have achieved fast and accurate segmentation, overcoming the reflection problem [60].

The iris texture extraction step is performed using techniques such as discrete cosine transform, Fourier transform, Haar wavelet, Gabor filter, etc. [61, 56]. Santos et al. In [62] a synthesis scheme was proposed to exploit different extraction techniques. The results show that the fusion approach can reduce the sensitivity of the system to low-quality data. This contribution is related to building systems in a less invasive way. Other image-based biometric systems include fingerprint or handprint recognition [63, 64, 65], hand geometry [66], dental biometrics [67], ear biometrics [68], millimetre-wave scans [69].

Multi modal biometrics is another area of current research. The idea of multi modal or hybrid biometrics is to combine different approaches to improve the aspects listed at the beginning of this section. 3. Many studies are developing statistical tools to efficiently extract and combine features from various sources, such as facial images and handprint scans [70]. Other recent studies include features at grade or classification level [71, 72, 73, 74]. Computational tools such as particle swarm optimization [75] are also used to optimize the fusion step.

3.8 Biometric Image Security:

Biometric records need to be correctly secured, however biometrics additionally provides a extensive array of safety functions (e.g. e-passport [41,82]). However, there are extensive protection issues concerning the saved biometric data. The use of biometric elements like face pix or fingerprints to beautify traditional cryptographic or watermarking structures is a promising approach. This lookup subject matter open some concerns: What takes place if the biometrics of a concern are stolen? What is the acceptable stability between overall performance and robustness? What biometric strategy need to we use in phrases of acceptable universality, distinctiveness, social acceptance, etc.? One of the strategies is to invulnerable biometric pictures by encryption techniques. These techniques once in a while operate lossy techniques over the photographs [76, 77]. Generally these structures have to decrypt the facts in order to proceed to the authentication process.

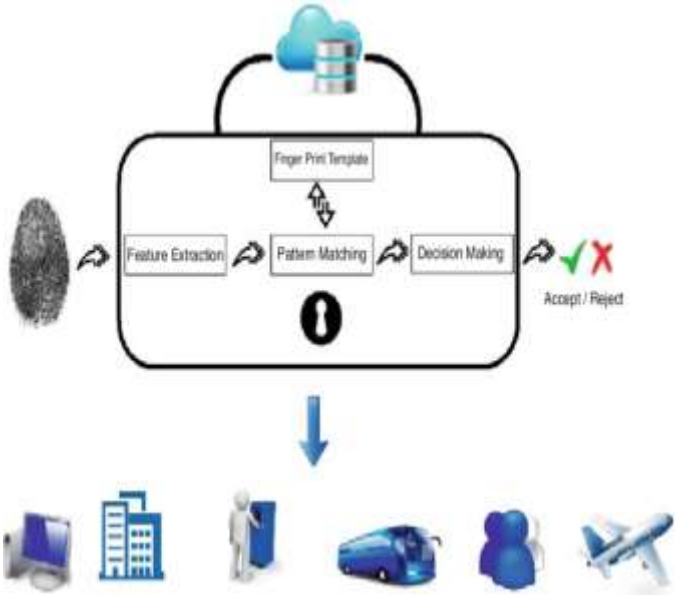

Fig. 3.3 Biometric Image Security

The undertaking of bio-cryptography is to put in force cancelable biometrics [78], which can be described as the software of non-invertible and repeatable adjustments to the authentic biometric templates. Steganography [34] and watermarking [79,80] are additionally being employed on biometric records security. This method approves embedding giant quantities of biometric records inside an image. Steganography can be employed to embed biometric photos into publicly transmitted photographs [34]. Multimodal biometric photograph watermarking is additionally a promising lookup region [81,11].

4 CONCLUSION:

Computer imaginative and prescient and imaging sciences are intently associated to biometrics. The interaction between each lookup areas is constantly evolving. Old biometric structures which relied on human visible verification are being displaced by using the gold standard inspecting skills of computers. Image records have emerge as an asset to protect, and we additionally use imaging methods to impervious data. Thus, new computational advances in steganography, watermarking or sample cognizance improve the improvement of invulnerable and advantageous biometric systems.

Similarly, ever-growing requirement of trustable biometrics by using governments and industry require regular lookup in such areas

References:

1. Petitcolas, F., Anderson, R., Kuhn, M.: Information hiding - a survey. Proceedings of the IEEE 87(7), 1062–1078 (1999)
2. Yang, C.N., Chen, T.S.: Colored visual cryptography scheme based on additive color mixing. Pattern Recognition 41(10), 3114–3129 (2008)
3. Yang, C.N., Ciou, C.B.: Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. Image and Vision Computing 28(12), 1600–1610 (2010)
4. Jin, J., Wu, Z.-H.: 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)
5. Tremeau, A., Muselet, D.: Recent trends in color image watermarking. Journal of Imaging and Science Technology 53(1), 010201 (2009)
6. Cox, I., Miller, M., Bloom, J.: Watermarking applications and their properties. In: Proceedings of International Conference on Information Technology: Coding and Computing, pp. 6–10 (2000)
7. Mahdian, B., Saic, S.: A bibliography on blind methods for identifying image forgery. Signal Processing-Image Communication 25(6), 389–399 (2010)
8. Xu, D., Wang, R., Wang, J.: A novel watermarking scheme for h.264/avc video authentication. Signal Processing-Image Communication 26(6), 267–279 (2011)
9. Kim, J., Kim, N., Lee, D., Park, S., Lee, S.: Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents. Signal Processing-Image Communication 25(8), 559–576 (2010) 10. Tsai, H.M., Chang, L.W.: Secure reversible visible image watermarking with authentication. Signal Processing-Image Communication 25(1), 10–17 (2010)
11. Vatsa, M., Singh, R., Noore, A.: Feature based rdwt watermarking for multimodal biometric system. Image and Vision Computing 27(3), 293–304 (2009)
12. Wang, K., Lavoue, G., Denis, F., Baskurt, A.: A comprehensive survey on three-dimensional mesh watermarking. IEEE Transactions on Multimedia 10(8), 1513–1527 (2008)
13. Darwish, A., Abraham, A.: The use of computational intelligence in digital watermarking: Review, challenges, and new trends. Neural Network World 21(4), 277–297 (2011)
14. Cancellaro, M., Battisti, F., Carli, M., Boato, G., Natale, F.D., Neri, A.: 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. Mostefa, I.B., Braci, S., Delpha, C., Boyer, R., Khamadja, M.: Quantized based image watermarking in an independent domain. Signal Processing-Image Communication 26(3), 194–204 (2011)
16. Chen, W.C., Wang, M.S.: A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. Expert Systems With Applications 36(2), 1300–1307 (2009)
17. Huang, H.C., Chu, C.M., Pan, J.S.: The optimized copyright protection system with genetic watermarking. Soft Computing 13(4), 333–343 (2009); 2nd IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, CA (2006)
18. Deng, C., Gao, X., Li, X., Tao, D.: A local tchebichef moments-based robust image watermarking. Signal Processing 89(8), 1531–1539 (2009) 444 I. Marqués and M. Graña
19. Chang, C.C., Chen, K.N., Lee, C.F., Liu, L.J.: A secure fragile watermarking scheme based on chaos-and-hamming code. Journal of Systems and Software 84(9), 1462–1470 (2011)
20. Chang, C.C., Lin, P.Y.: Adaptive watermark mechanism for rightful ownership protection. Journal of Systems and Software 81(7), 1118–1129 (2008)
21. Cintra, R.J., Dimitrov, V.S., de Oliveira, H.M., Campello de Souza, R.M.: Fragile watermarking using finite field trigonometrical transforms. Signal Processing-Image Communication 24(7), 587–597 (2009)
22. Zhang, X., Wang, S.: Fragile watermarking scheme using a hierarchical mechanism. Signal Processing 89(4), 675–679 (2009)
23. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory 22, 644–654 (1976)
24. Hwang, H.-E.: An optical image cryptosystem based on hartley transform in the fresnel transform domain. Optics Communications 284(13), 3243–3247 (2011)
25. Zhou, N., Wang, Y., Wu, J.: Image encryption algorithm based on the multi-order discrete fractional mellin transform. Optics Communications 284(24), 5588–5597 (2011)
26. Zhong, Z., Chang, J., Shan, M., Hao, B.: Fractional fourier-domain random encoding and pixel scrambling technique for double image encryption. Optics Communications 285(1), 18–23 (2012)
27. Lin, Q.H., Yin, F.L., Mei, T.M., Liang, H.: A blind source separation-based method for multiple images encryption. Image and Vision Computing 26(6), 788–798 (2008)
28. Ulutas, M., Ulutas, G., Nabiyev, V.V.: Medical image security and epr hiding using shamir's secret sharing scheme. Journal of Systems and Software 84(3), 341–353 (2011)
29. Cheddad, A., Condell, J., Curran, K., Kevitt, P.M.: Digital image steganography: Survey and analysis of current methods. Signal Processing 90(3), 727–752 (2010)
30. Kim, K.S., Lee, M.J., Lee, H.Y., Lee, H.K.: Reversible data hiding exploiting spatial correlation between sub-sampled images. Pattern Recognition 42(11), 3083–3096 (2009)
31. Tai, W.L., Yeh, C.M., Chang, C.C.: Reversible data hiding based on histogram modification of pixel differences. IEEE Transactions on Circuits and Systems for Video Technology 19(6), 904–908 (2009)
32. Braci, S., Delpha, C., Boyer, R.: How quantization based schemes can be used in image steganographic context. Signal Processing-Image Communication 26(8-9), 567–576 (2011)
33. Tseng, H.W., Hsieh, C.P.: Prediction-based reversible data hiding. Information Sciences 179(14), 2460–2469 (2009)
34. Qi, M., Lu, Y., Du, N., Zhang, Y., Wang, C., Kong, J.: A novel image hiding approach based on correlation analysis for secure multimodal biometrics. Journal of Network and Computer Applications 33(3), 247–257 (2010)
35. Chang, C.C., Lee, J.S., Le, T.H.N.: Hybrid wet paper coding mechanism for steganography employing n-indicator and fuzzy edge detector. Digital Signal Processing 20(4), 1286–1307 (2010) 36. Wu, C.C., Kao, S.J., Hwang, M.S.: A high quality image sharing with steganography and adaptive authentication scheme. Journal of Systems and Software 84(12), 2196–2207 (2011)
37. Zhao, H., Wang, H., Khan, M.K.: Steganalysis for palette-based images using generalized difference image and color correlogram. Signal Processing 91(11), 2595–2605 (2011) Image Security and Biometrics: A Review 445
38. Chao, M.W., Lin, C.H., Yu, C.W., Lee, T.Y.: A high capacity 3d steganography algorithm. IEEE Transactions on Visualization and Computer Graphics 15(2), 274–284 (2009)
39. Amat, P., Puech, W., Druon, S., Pedeboy, J.P.: Lossless 3d steganography based on mst and connectivity modification. Signal Processing-Image Communication 25(6), 400–412 (2010)
40. Elsheh, E., Hamza, A.B.: Secret sharing approaches for 3d object encryption. Expert Systems with Applications 38(11), 13906–13911 (2011)
41. Schouten, B., Jacobs, B.: Biometrics and their use in e-passports. Image and Vision Computing 27(3), 305–312 (2009)
42. Jain, A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology 14(1), 4–20 (2004)
43. Biometric technology today, vol. 2011 (2011)
44. Chellappa, R., Sinha, P., Phillips, P.J.: Face recognition by computers and humans. IEEE Computer 43(2), 46–55 (2010)
45. Shan, C., Gong, S., McOwan, P.W.: Facial expression recognition based on local binary patterns: A comprehensive study. Image and Vision Computing 27(6), 803–816 (2009)

46. Gui, J., Jia, W., Zhu, L., Wang, S.L., Huang, D.S.: Locality preserving discriminant projections for face and palmprint recognition. Neurocomputing 73(13-15), 2696–2707 (2010)
47. Wan, M., Lai, Z., Shao, J., Jin, Z.: Two-dimensional local graph embedding discriminant analysis (2dlgeda) with its application to face and palm biometrics. Neurocomputing 73(1-3), 197–203 (2009)
48. Marques, I., Graña, M.: Face recognition with lattice independent component analysis and extreme learning machines. Soft Computing (in press)
49. Qiao, L., Chen, S., Tan, X.: Sparsity preserving projections with applications to face recognition. Pattern Recognition 43(1), 331–341 (2010)
50. Wright, J., Yang, A.Y., Ganesh, A., Sastry, S.S., Ma, Y.: Robust face recognition via sparse representation. IEEE Transactions on Pattern Analysis and Machine Intelligence 31(2), 210–227 (2009)
51. Zhang, T., Fang, B., Yuan, Y., Tang, Y.Y., Shang, Z., Li, D., Lang, F.: Multiscale facial structure representation for face recognition under varying illumination. Pattern Recognition 42(2), 251–258 (2009)
52. Marcialis, G.L., Roli, F., Muntoni, D.: Group-specific face verification using soft biometrics. Journal of Visual Languages and Computing 20(2), 101–109 (2009)
53. Hollingsworth, K., Bowyer, K.W., Flynn, P.J.: Useful features for human verification in near-infrared periocular images. Image and Vision Computing 10.1016/j.imavis.2011.09.002(0) (2011)
54. Pan, Z., Healey, G., Prasad, M., Tromberg, B.: Face recognition in hyperspectral images. IEEE Transactions on Pattern Analysis and Machine Intelligence 25(12), 1552–1560 (2003)
55. Efraty, B., Bilgazyev, E., Shah, S., Kakadiaris, I.A.: Profile-based 3d-aided face recognition. Pattern Recognition 45(1), 43–53 (2012)
56. Bowyer, K.W., Hollingsworth, K., Flynn, P.J.: Image understanding for iris biometrics: A survey. Computer Vision and Image Understanding 110(2), 281–307 (2008) 57. Hollingsworth, K., Bowyer, K.W., Lagree, S., Fenker, S.P., Flynn, P.J.: Genetically identical irises have texture similarity that is not detected by iris biometrics. Computer Vision and Image Understanding 115(11), 1493–1502 (2011) 446 I. Marqués and M. Graña
58. Hollingsworth, K., Bowyer, K.W., Flynn, P.J.: Pupil dilation degrades iris biometric performance. Computer Vision and Image Understanding 113(1), 150–157 (2009)
59. Baker, S.E., Hentz, A., Bowyer, K.W., Flynn, P.J.: Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. Computer Vision and Image Understanding 114(9), 1030–1044 (2010)
60. He, Z., Tan, T., Sun, Z., Qiu, X.: Toward accurate and fast iris segmentation for iris biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence 31(9), 1670–1684 (2009) 61. Kumar, A., Passi, A.: Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognition 43(3), 1016–1026 (2010)
62. Santos, G., Hoyle, E.: A fusion approach to unconstrained iris recognition. Pattern Recognition Letters 10.1016/j.patrec.2011.08.017(0) (2011)
63. Amayeh, G., Bebis, G., Erol, A., Nicolescu, M.: Hand-based verification and identification using palm-finger segmentation and fusion. Computer Vision and Image Understanding 113(4), 477–501 (2009) 64. Chen, J., Moon, Y.S., Wong, M.F., Su, G.: Palmprint authentication using a symbolic representation of images. Image and Vision Computing 28(3), 343–351 (2010)
65. Kong, A., Zhang, D., Kamel, M.: A survey of palmprint recognition. Pattern Recognition 42(7), 1408–1418 (2009) 66. Nicolae, D.: A survey of biometric technology based on hand shape. Pattern Recognition 42(11), 2797–2806 (2009)
67. Lin, P.L., Lai, Y.H., Huang, P.W.: Dental biometrics: Human identification based on teeth and dental works in bitewing radiographs. Pattern Recognition 45(3), 934–946 (2012)
68. Arbab-Zavar, B., Nixon, M.S.: On guided model-based analysis for ear biometrics. Computer Vision and Image Understanding 115(4), 487–502 (2011)
69. Alefs, B., den Hollander, R., Nennie, F., van der Houwen, E., Bruijn, M., van der Mark, W., Noordam, J.: Thorax biometrics from millimetre-wave images. Pattern Recognition Letters 31(15), 2357–2363 (2010) 70. Xu, Y., Zhang, D., Yang, J.Y.: A feature extraction method for use with bimodal biometrics. Pattern Recognition 43(3), 1106–1115 (2010)
71. Xu, Y., Zhu, Q., Zhang, D.: Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments. Neurocomputing 74(18), 3946–3952 (2011)
72. Marcialis, G.L., Roli, F., Didaci, L.: Personal identity verification by serial fusion of fingerprint and face matchers. Pattern Recognition 42(11), 2807–2817 (2009)
73. Alsaade, F., Ariyaeeinia, A., Malegaonkar, A., Pillay, S.: Qualitative fusion of normalised scores in multimodal biometrics. Pattern Recognition Letters 30(5), 564–569 (2009)
74. Hanmandlu, M., Grover, J., Gureja, A., Gupta, H.: Score level fusion of multimodal biometrics using triangular norms. Pattern Recognition Letters 32(14), 1843–1850 (2011)
75. Raghavendra, R., Dorizzi, B., Rao, A., Kumar, G.H.: Designing efficient fusion schemes for multimodal biometric systems using face and palmprint. Pattern Recognition 44(5), 1076–1088 (2011)
76. Bhatnagar, G., Wu, J., Raman, B.: Fractional dual tree complex wavelet transforms and its application to biometric security during communication and transmission. Future Generation Computer Systems 28(1), 254–267 (2012) Image Security and Biometrics: A Review 447
77. Acharya, B., Sharma, M.D., Tiwari, S., Minz, V.K.: Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem. Procedia Computer Science 2(0), 242–247 (2010)
78. Bolle, R.M., Connell, J.H., Ratha, N.K.: Biometric perils and patches. Pattern Recognition 35(12), 2727–2738 (2002)
79. Lee, H., Lim, J., Yu, S., Kim, S., Lee, S.: Biometric image authentication using watermarking. In: International Joint Conference on SICE-ICASE 2006, pp. 3950 –3953 (2006)
80. Allah, M.M.A.: Embedded biometric data for a secure authentication watermarking. In: Proceedings of the Fourth conference on IASTED International Conference: Signal Processing, Pattern Recognition, and Applications, Anaheim, CA, USA, pp. 191–196. ACTA Press (2007)
81. Kim, W.G., Lee, H.: Multimodal biometric image watermarking using two-stage integrity verification. Signal Processing 89(12), 2385–2399 (2009)
82. Dr. D. Kannan and Mrs. P. Shobana.:Survey based on image security using Various methodologies under networking system. International Journal of Research and Analytical Reviews, 9(1), 2349-5138. (2022)