Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Survey on Biometrics based Digital Image Watermarking Techniques and Applications

D. Kannan[1]

[1] Cikkanna Govt. Arts College/Bharathiar University

Received: 8 December 2012 Accepted: 1 January 2013 Published: 15 January 2013

Abstract

The improvements in Internet technologies and growing demands on online multimedia businesses have made digital copyrighting as a major challenge for businesses that are associated with online content distribution via diverse business models including pay-per-view, subscription, trading, etc. Copyright protection and the evidence for rightful ownership are major issues associated with the distribution of any digital images. Digital watermarking is a probable solution for digital content owners that offer security to the digital content. In recent years, digital watermarking plays a vital role in providing the apposite solution and numerous researches have been carried out. In this paper, an extensive review of the prevailing literature related to the Bio- watermarking is presented together with classification by utilizing an assortment of techniques. In addition, a terse introduction about the Digital Watermarking is presented to get acquainted with the vital information on the subject of Digital Watermarking.

Index terms— digital watermarking, image watermarking, watermark, copy right protection, visible watermarking, invisible watermarking, spatial domain, transform do

1 Introduction

n the information-oriented society, sounds, images, and videos are the various needs in the media form for protecting the information. Apart from of its media forms, the majority information is distributed as digital signals, especially via networks such as the Internet [1]. While the initiation of digital multimedia enables the creation and distribution of products swiftly via electronic means the rapid growth of the Internet makes communication easier and more extensive than before [2]. In current era, the rapid expansion of the interconnected networks [3] and the never-ending development of digital technologies have facilitated instant multimedia transmission and the creation of large-scale digital image databases [4]. The advantages of digitized images are that without considerable loss of quality, images can be easily manipulated and reproduced [6]. Nevertheless, these also entail that with malicious intentions [5] images can be modified easily and invisibly.

The utmost utilization of the interconnected networks for instantaneous transaction prevail and the power of digital multimedia processing tools for perfect duplication and manipulation augments, forgery and impersonation [8] turn out to be major concerns of the information era [7]. Especially when the media content is critical, the situation can be very stern for instance, once an image has been exploited as a part of evidence in the court, there has to be some ways to prove that the image is original or the semantics of the original image is well maintained. Such an application is considered as content authentication [11]. In the last decade, in response to these confronts, approaches conveying the authentication data in digital media have been proposed [7]. Hence the fortification and enforcement of intellectual property rights for digital media has become a significant issue [9] and therefore a few work requests to be made to extend security systems to protect the content of digital data [10].

Digital Rights Management (DRM) is one among the potential solutions for the abovementioned issue. DRM is a technique recognized by the administrators of the intellectual assets, such as license terms and usage agreements

for honoring copyright provisions. The DRM comprises a set of technologies that are exploited by establishing privileges, specifically by means of content protection to put off exploitation of the digital content [12]. DRM is a compilation of technologies that provides content protection according to granted rights by enforcing the utilization of digital content. To protect their copyrights, it enables content owners and content providers and maintains control over distribution of and access to content [13].

The encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hard-and software, key management and revocation as well as risk management architectures are also comprised in technologies which in turn applied for the DRM [14]. To achieve rights management, Digital watermarking is a promising technology employed by a variety of Digital Rights Management (DRM) systems. It aids copyright information (such as the owner's identity, transaction dates, and serial numbers) to be embedded as insignificant signals into digital contents [15]. Digital watermarking has observed rapid escalation in recent times [16].

In the past few years, several researches are performed in the digital watermarking by a huge number of researchers. In this paper, we present a comprehensive review of extremely important researches on Digital image watermarking together with their processing and analysis methods. The popular literature existing in the digital image watermarking is categorized and reviewed comprehensively. Here, we present a wide-ranging review of image watermarking which is robust against diverse attacks. A broad review on the study of significant research methods in Digital Image Watermarking is presented in section.

2 Literature Survey

Both watermarking and cryptography are necessary for effective Digital Rights Management (DRM) of multimedia in the framework of embedded systems have presented a system in the form of a digital camera has been presented by Mohamed Zuhair et al. [17] which embeds biometric data into an image. In the digital camera, they have incorporated both the encryption and watermarking together that has been assisted for protecting and authenticating image files and Watermarking the digital content with origin information or intended recipient identification secures content from electronic data theft. An invisible watermarking algorithm has been employed which allows verification of the image as well as the identity of the carrier. Towards the development of the complete digital camera, they have presented architecture and hardware efficient FPGA based invisible watermark module.

When compared with the conventional personal identification approaches such as passwords and PIN codes, automated biometrics authentication offers a suitable and reliable technique in diverse applications, but their validity must be assured. Watermarking approaches may be a solution to assure the validity of biometrics. In this paper, a new approach of protecting hidden transmission of biometrics using authentication watermarking is proposed by Shum in Ding et al., [18]. Five watermark bits constructed from each DCT block are split into two segments such as authentication bits and hidden bits. The four authentication bits are used to verify the reliability of each image block; the hidden bit is used as a hidden channel to transmit the biometric data. At the receiver, the reliability of each block is verified through authentication watermarking. The biometrics data is derived from the block which has been noticed as innocent. Redundancy embedding and voting approach are utilized as improving the correctness of extracte biometrics data. Theoretical analysis and experimental results reveal that the proposed approach protects hidden transmission of biometrics and can competently recover the biometrics when the watermarked-images suffer from malicious tamper.

Digital rights management (DRM) system is the significant approach for digital transactions. An efficient authentication approach of DRM system for remote users based on multimodal biometrics (such as iris and face feature) verification and watermarking and smart cards is proposed by Desong Wang et al., [19], which comprises of two authentication phases, i.e. the client server authentication and the server authentication. For the client server authentication, the author combine watermarking technique and multimodal biometric system depending on extremely secure iris recognition and face recognition to offer more secure and reliable personal recognition. In watermarking algorithm, face image is selected to be the host image, iris feature is chosen to use as watermark hidden in the host face image. For the server authentication, the proposed approach is an extended and generalized form of ElGamal signature approach whose security depends on discrete logarithm problem, which is not yet forged. So, the proposed technique can attain the rights management of digital content exactly using the illegal user access control. In the meantime, the bimodal biometrics (iris and face) recognition offers the enhancement in the accuracy performance of the system.

The strong advancement of digital technologies has demanded the owners to pay immense attention in securing their digital contents. Recently, watermarking has been exploited by researchers for the security of digital documents. But, the embedded watermark data can be hacked by the hackers and therefore it is a threat to protection of digital content. This approach by Rao et al., [20] is an efficient approach for protecting the copyrights of digital images with the integration of both biometrics and digital watermarking. The proposed approach exploits the fingerprint biometric feature of the proprietor to generate the watermark. The minutiae points are attained from the fingerprint and the coordinates of the minutiae points are shuffled. Then, a vector is generated from the shuffled coordinates of minutiae points and is ultimately used as watermark.

The embedding and extraction of watermark is executed in the DCT-SVD domain. If any ownership clashes arise on the image, the watermark is obtained from the watermarked image and assessed against the vector

generated from the shuffled co-ordinates of minutiae points which are attained from the fingerprint of the person asserting ownership. If they go with each other, the claiming person is considered to be the rightful owner of the image. Thus, the biometric feature used in this scheme establishes that the information is very safe. Moreover, it is not necessary to execute the information; it is not possible for the hackers to hack it as well.

A novel authentication approach to set up Digital Rights Management (DRM) based on multimodal biometric verification and watermarking technique is proposed Edward et al., [21]. The biometric features used in this approach are iris and face. In this watermark, face image is considered to be the host image and the iris feature is chosen as the watermark hidden in the host image. Such that, iris feature watermark not only defend face biometric data but also can be utilized as covert recognition. The transformation utilized for watermark is ridgelet transform. The embedding is carried out based on the HVS characteristic features. In this consideration, data is embedded based on two usual perceptual rules disturbances that are less visible in the highly textured regions, and they are more easily apparent around edges than in textured areas, but less easily than in uniform regions. The data is embedded based on these rules. Initially, enrollment process of the victim face and iris features in the available database. Secondly, authentication process is carried out through comparing the features of face image with the features of the face image in the data base. When it matches the iris feature is compared with data base if the iris image is also matched then the person is authenticated. This type of biometric provides better authentication and security.

Bio-watermarking systems were proposed as the synergistic integration of biometrics and digital watermarking to guarantee the integrity, authenticity and confidentiality of digitized image documents, and biometric templates. The influence of watermarking attacks on the performance of offline signature verification is evaluated in the context of significant biowatermarking systems. The considered system depends on incremental learning computational intelligence, and multi-objective formulation that facilitates optimizing parameters based on watermark quality and robustness simultaneously. In this approach by Rabil et al., [22], Extended Shadow Code features are obtained from digitized offline signatures, collected into feature vectors, and discretized into binary watermarks preceding to being embedded into high resolution grayscale face image. The influence on biometric verification performance of quantization and different intensities of attacks are taken into account, and the effect of using only some areas of face images of higher texture Region Of Interest (ROI) for embedding the watermark is also observed. Experimental results reveal the optimal discretization, and better watermark fitness and verification performance when embedding in ROI. In order to enhance the performance, more reference signatures are to be embedded, efficient ROI identification approaches have to be used and finally novel formulation to add biometrics verification fitness to the watermark quality and robustness fitness during embedding optimization. The proposed system can be used to verify individuals crossing borders using offline signatures, or protecting biometric templates.

Biometrics security technique using wavelet based watermarking is proposed by Jong Gook Ko et al., [23]. Two types of techniques are presented that increase privacy protection level. First technique is to embed ID watermark data to biometric image like fingerprint, face for backtracking when image missing. Secondly, as multi bio watermarking, fingerprint feature data are embedded to face image for hiding private biometric information. The proposed technique for bio watermarking depends on the wavelet transform and reduces recognition performance loss owing to watermark data embedding.

[24] Liu Hui et al., [24] proposed a novel biometrics watermarking approach in the host as notice of genuine. In the watermark embedding process, the wavelet coefficients of the host image are assembled into wavelet trees and each watermark bit is embedded using two trees. The trees are so quantized that they show a large adequate statistical difference, which will later be used for watermark extraction. The experimental results reveal that the proposed approach is effective and robust to common image processing functions and some geometric operations such as JPEG compression, JPEG2000 compression, filtering, adding Gaussian noise and row-column removal.

Tuan Hoang et al., [25] proposed a multibiometrics authentication system depending on the proposed priority-based watermarking technique. Tuan Hoang et al., examined how the watermarking approach influence the container, which is facial image exploited in additional authentication steps. The author conducted experiments on facial and fingerprint features by means of both priority-based watermarking technique and nonpriority-based technique. It is revealed that the proposed priority-based watermarking technique has minimized data retrieval errors from the facial image after decoding, thus it has also minimized authentication error rates.

Cheng-Yaw et al., [26] presented a novel biometric watermarking approach to embed handwritten signature invisibly in the host as a sign of genuine ownership. The author proposed to adaptively integrate Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT) approaches into a unison framework, which to be known as LSB-DWT approach. The performance of LSB-DWT approach is evaluated against simulated frequency and geometric attacks, particularly JPG compression, low pass filtering, median filtering, noise addition, scaling, rotation and cropping through visual inspection, Peak Signal to Noise Ratio (PSNR) and watermark distortion rate. The experiment results show that LSB-DWT approach is effectively robust even in the existence of calculated distortions.

Vatsa et al., [27] presented a multimodal biometrics system using watermarking approach with two levels of security for concurrently verifying an individual and protecting the biometric template. Iris template is watermarked in face, such that the face is visible for verification and the watermarked iris is used to cross

authenticate the individual and secure the biometrics data as well. The accuracy of the multimodal biometrics system is around 96.8%. This approach is(D D D D D D D D)

Year also resistant to common attacks on biometric templates.

Tuan Hoang et al., [28] proposed a novel remote multimodal biometric authentication structure based on fragile watermarking for transmitting multibiometrics over networks to server for authentication. A facial image is exploited as a container to embed other numeric biometrics features. The proposed framework improves security and minimizes bandwidths. To minimize error rates from embedding numeric data, the author proposed a new technique to find out bit priority level in a bit sequence denoting the numerical information to be embedded and integrate with the present amplitude modulation watermarking technique.

Kang Hui et al., [29] proposed an approach based on the fingerprint watermark, and attempt to establish biometrics in the watermark system. The author wished to combine the digital watermarking technology with the fingerprint identification technology. The approach depends upon the spatial domain, DCT domain of multi-bits embedded watermark techniques to embed and obtain the information of the fingerprint characteristic, and it is better to obtain the simplicity in the robustness and embedded technique. The experiment has revealed the fact that the approach is feasible and effective.

3 Direction for the Future Research

In this review paper, numerous Biowatermarking techniques utilized for the digital image watermarking have been analyzed thoroughly. In addition, the performance claimed by the Biowatermarking techniques has also been evaluated. As a result of this analysis, it has been evident that use biometrics data for digital image watermarking in copyright protection has given significant results. As biometric data are unique for each person, providing the biometrics data as the watermark has the potential to attain better results and may lead to the evolution of watermarking technique as a noteworthy research area. But, still advanced biometric techniques have to be incorporated with the watermarking technique for providing better security. This paper will be a healthier foundation for the budding researchers in the digital image watermarking domain to get acquainted with the techniques available in it.

4 Conclusion

Digital image watermarking is a rising research area that has received great attention from the research community over the past decade. In this paper, a comprehensive survey of the significant researches and techniques existing for digital watermarking has been scrutinized. Here, existing researches that are robust against attacks are analyzed. An introduction about the digital watermarking and its applications has also been presented and the existing researches are organized according to the techniques implemented. This survey paves the way to the budding researchers to know about the numerous techniques available for Biowatermarking.

Figure 1: FA

[Ding] , Shumin Ding .

[Ko] , Jong Gook Ko .

[Hui] , Liu Hui .

[Hoang] , Tuan Hoang .

[Tran] , Dat Tran .

[Sharma and Trung Le] , D Sharma , Trung Le .

[Low] , Cheng-Yaw Low .

[Teoh and Beng-Jin] , Andrew Teoh , Beng-Jin .

[Hoang] , Tuan Hoang .

[Tran] , Dat Tran .

[Hui] , Kang Hui .

[Jing] , Liu Jing .

[Xiao-Dong] , Zhu Xiao-Dong .

[Chen et al. ()] 'A communication system model for digital image watermarking problems'. Pei-Chun Chen , Yung-Sheng Chen , Wen-Hsing Hsu . *International Journal of Computer Science* 2007. 34 (2) .

[Dorairangaswamy (2009)] 'A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection'. Dorairangaswamy . *International Journal of Engineering and Technology* August 2009. 1 (3) p. .

[Chung and Xu ()] 'A Secure Digital Watermarking Scheme for MPEG-2 Video Copyright Protection'. Yuk Ying Chung , Fang Fei Xu . *2006 IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS'06)*, 2006. p. .

[Rao et al. ()] 'An efficient copyright protection scheme for digital images using biometrics and watermarking'. N N Rao , P Thrimurthy , B R Babu . *2nd IEEE International Conference on Computer Science and Information Technology*, (Page(s) 2009. p. .

[Cao et al. (2001)] 'An Image-Adaptive Watermark Based On A Redundant Wavelet Transform'. Jian-Guo Cao , James E Fowler , Nicholas H Younan . *proceedings of IEEE International Conference on Image Processing*, (IEEE International Conference on Image ProcessingThessaloniki, Greece) October 2001. p. .

[Wang and Li; Memik ()] 'Authentication Scheme of DRM System for Remote Users Based on Multimodal Biometrics, Watermarking and Smart Cards'. Desong Wang , ; Jianping Li; Memik , G . *WRI Global Congress on Intelligent Systems, GCIS '09*, (Page(s) 2009. p. .

[Moon ()] 'Biometrics Security Scheme for Privacy Protection'. Ki Young Moon . *Advanced Software Engineering and Its Applications (ASEA)*, (Page(s) 2008. p. .

[Taskovski et al. ()] 'Blind Low Frequency Watermarking Method'. Dimitar Taskovski , Sofija Bogdanova , Momcilo Bogdanov . *International Journal of Signal Processing* 2006. 2 (3) p. .

[Diplomarbeit ()] *Digital image watermarking in the wavelet transform*, Diplomarbeit . 2001. (Technical Report)

[Vatsa et al. ()] 'Digital watermarking based secure multimodal biometric system'. M Vatsa , R Singh , P Mitra , A Noore . *IEEE International Conference on Systems, Man and Cybernetics*, (Page(s) 2004. p. .

[Li ()] *Digital watermarking schemes for multimedia authentication*, Chang-Tsun Li . 2005. Idea Group Publishing. p. .

[Zolghadrasli (2007)] 'Evaluation of spread spectrum watermarking shemes in the wavelet domain using HVS characteristics'. Rezazadeh Zolghadrasli . *proceedings of 9th International Symposium on Signal Processing and its Applications*, (9th International Symposium on Signal Processing and its ApplicationsSharjah) February 2007.

[Zuhair and Yousuf ()] 'FPGA Based Image Security and Authentication in Digital Camera using Invisible Watermarking Technique'. Mohamed Zuhair , Mohamed Yousuf . *International Journal of Engineering Science and Technology* 2010. 2 (6) p. .

[Kumhom and On (2004)] 'Image Watermarking Based On Wavelet Packet Transform With Best Tree'. Kumhom , - On , Chamnongthai . *ECTI Transactions on Electrical Eng. Electronics and Communications* February 2004. 2 (1) p. .

[Rabil et al. ()] 'Impact of watermarking on offline signature verification in intelligent bio-watermarking systems'. B S Rabil , R Sabourin , E Granger . *IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM)* 2011. p. .

[Conrado and Petkovic (2006)] 'Michiel van der Veen and Wytse van der Velde "Controlled Sharing of Personal Content Using Digital Rights Management'. Claudine Conrado , Milan Petkovic . *Journal of Research and Practice in Information Technology* February 2006. 38 (1) p. .

[Edward et al. ()] 'Person authentication using multimodal biometrics with watermarking'. S Edward , S Sumathi , R Ranihemamalini . *International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN)*, (Page(s) 2011. p. .

[Le ()] 'Priority Watermarking-Based Face-Fingerprint Authentication System'. B H Le . *International Conference on Information and Multimedia Technology, ICIMT '09*, (Page(s) 2009. p. .

[Li and Liu ()] 'Protecting Hidden Transmission of Biometrics Using Authentication Watermarking'. Chunlei Li , ; Zhoufeng Liu . *WASE International Conference on Information Engineering (ICIE)*, (Page(s) 2010. p. .

[Tang and Hung ()] 'Recoverable Authentication of Wavelet-Transformed Images'. Yuan-Liang Tang , Chih Jung Hung . *ICGST/GVIP Special Issue on Watermarking* 2007. 7 p. .

[Sharma ()] 'Remote multimodal biometric authentication using bit priority-based fragile watermarking'. D Sharma . *19th International Conference on Pattern Recognition, ICPR*, (Page(s) 2008. p. .

[El-Taweel et al. ()] 'Secure and Non-Blind Watermarking Scheme for Color Images Based on DWT'. El-Taweel , Onsi , Darwish Samy . *Vision and Image Processing*, 2005. 5 p. . (GVIP))

[Tee ()] Connie Tee . *Fusion of LSB and DWT Biometric Watermarking for Offline Handwritten Signature*, (Page(s) 2008. p. . (Congress on Image and Signal Processing, CISP '08)

[Bechtold ()] 'The present and Future of Digital Rights Management'. Stefan Bechtold . *proceedings of Second International Conference on Automated Production of Cross Media Content for multi-channel Distribution*, (Second International Conference on Automated Production of Cross Media Content for multi-channel Distribution) 2003.

[Cheung et al. (2008)] 'The Use of Digital Watermarking for Intelligence Multimedia Document Distribution'. Shing-Chi Cheung , K W Dickson , Cedric Chiu , Ho . *Journal of Theoretical and Applied Electronic Commerce Research* December 2008. 3 (3) p. .

[Li and Si (2007)] 'Wavelet based Fragile Watermarking scheme for image authentication'. Chang-Tsun Li , Huayin Si . *Journal of Electronic Imaging* March 2007. 16 (1) p. .

[Yu-Ping ()] 'Wavelet Tree Quantization-Based Biometric Watermarking for Offline Handwritten Signature'. Hu Yu-Ping . *International Asia Symposium on Intelligent Interaction and Affective Computing ASIA '09*, (Page(s) 2009. p. .

[Tian ()] 'Wavelet-based reversible watermarking for authentication'. Jun Tian . *In proceedings of SPIE* 2002. 4675 p. .

[Xiao-Xu ()] Zhang Xiao-Xu . *International Conference on Computer Science and Software Engineering*, (Page(s) 2008. p. . (Study on Implementation of a Fingerprint Watermark)