International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

RESEARCH ARTICLE

ISSN: 2321-7758

AN OVERVIEW OF BIO-METRIC BASED DIGITAL WATERMARKING TECHNIQUES AND APPLICATIONS

PRIYANKA JAWALE[1], Dr. P. M. MAHAJAN[2]

[1]M. E. Student,

[2]J. T. Mahajan College of Engg. Faizpur

ABSTRACT

Implementation of new approach of image watermarking algorithm with integration of the Singular value decomposition and discrete wavelet transform is proposed in this paper, considering main purpose to enhance multimedia data security and DC coefficient for performance analysis of implemented algorithm. Implementation of the algorithm with integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. Thus this scheme provides a securerobust and imperceptible watermarking technology in total. In recent years, digital watermarking plays a vital role in providing the best solution in copyrights and numerous researches have been carried out in this area. A broad review of the general literature related to the Bio- watermarking is presented together with classification by utilizing a variety of techniques. In addition, a brief introduction about the Digital Watermarking is presented to get up to date with the important information on the subject of Digital Watermarking. Index Terms—digital watermarking, image watermarking, watermark, discrete wavelet transform (DWT), singular value decomposition (SVD), biometrics.

I. INTRODUCTION

In 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. 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. The advantages of digitized images are that without than before. In current era, the rapid expansion of the interconnected networks and the never-ending development of digital technologies have facilitated instant multimedia transmission and the creation of large-scale digital image databases considerable loss of quality, images can be easily manipulated and reproduced. Never the less, these also entail that with malicious intentions images can be modified easily and invisibly [1]. 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 turn out to be major concerns of the information era. Especially when the media content is critical, the situation can be very stern for instance, once an image has been ex-ploited 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 [2]. Such an application is considered as content authentication. In the last decade, in response to these confronts, approaches conveying the authentication data in digital media have been proposed. Hence the fortification and enforcement of intellectual property rights for digital media has become a significant issue and therefore a few work requests to be made to extend security systems to protect the content of digital data [3, 4]. 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. 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. The encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamperer-tant 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. 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 owners identity, transaction dates [5], and serial numbers) to be embedded as insignificant signals into digital contents. Digital watermarking has observed rapid escalation in recent times. 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 [6]. A broad review on the study of significant research methods in Digital Image Watermarking is presented in section. This paper is organized as follows. In Section II short review of related literature on proposed watermarking algorithm with SVD and DWT and finally we conclude about this work on the basis of obtained brief review of this field.

A. Biometrics Biometric technology uses the measurements of a unique human attribute or feature in order to distinguish that person from all others. Biometric authentication is categorized in to two major groups: physiological and behavioral characteristics as shown in figure 1. Behavioral Characteristics are biometric characteristics that are acquired over time by an individual, and are at least partly based on acquired behavior. Behavioral characteristics includes: gait, signature, voice and so on. Example of physiological characteristics includes DNA, ear Shape, face, fingerprint, hand geometry, iris, and retina. Physiological characteristics unlike behavioral characteristics cannot be simulated. So, physiological characteristics are more secured and popular than behavioral characteristics [4].

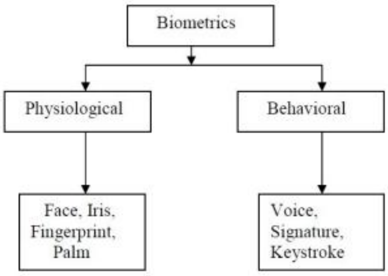

Fig. 1: Different types of biometrics

B. Watermarking: Watermarking is embedding information, which is able to show the ownership or track copy right-intrusion, into the digital image, video or audio. Its purpose determines that the watermark should be indivisible and robust to common processing and attack. Watermarking can be either visible or invisible. Visible watermark is used in images and videos but they tend to spoil the beauty and moreover the position of the watermark is disclosed to the attackers in this case. This led to the popularity of the invisible watermarking, where the Position of the watermark is not open to the public [19].

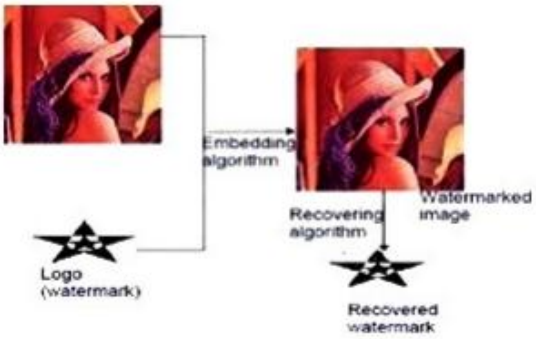

Fig. 2: Watermarked Image

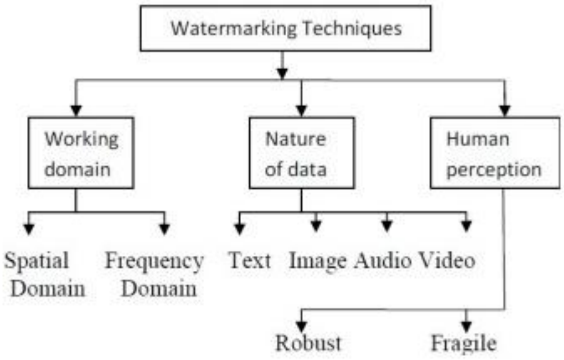

Fig. 3: Watermarking Techniques

II. LITERATURE SURVEY

R. Liu et al. [7] presented a digital watermarking algorithm based on singular value decomposition (SVD) technique as a solution to the problem of copyright protection of multimedia documents in networked environments. They has two important issues that watermarking algorithms need to address. First a schemes to provide trustworthy evidence for protecting rightful ownership and Second it should satisfy the requirement of robustness and resist distortions due to common image manipulations (such as filtering, Complex 2D Gabor filters compression, etc.). He compared his method with the Spread Spectrum Communication method proposed by Cox in order to put the performance investigation of his algorithm in proper context. The algorithm is tested on a variety of images, but for the sake of space, here he only gave the results obtained using the 200200 grayscale image Lena and test robustness under six practical conditions: adding noise, low-pass filtering, JPEG compression, scaling, image cropping, and rotation. Results showed that the new watermarking method performs well in both security and robustness. S. Mallat et al. [8] showed Multiresolution representations is very effective for analyzing the information content of images. This work showed the properties of the operator which approximates a signal at a given resolution and showed the difference of information between the approximation of a signal at the resolutions 2j+1 and 2j can be extracted by decomposing the signal. This decomposition defines an orthogonal multiresolution representation called a wavelet representation. It is computed with a pyramidal algorithm based on convolutions with quadrature mirror filters. For images, the wavelet representation differentiates spatial orientations. He studied the application of this representation to data compression in image coding, texture discrimination and fractal analysis. He calculated the ratios of the energy of the detail images within each orientation for the resolutions , 1/4 and 1/8. He recovered the fractal dimension of this image from each of these ratios with a 3 percent maximum error. R. Bodade, et al. [9] proposed aapproach of feature extraction of iris image using multi-directional wavelets obtained by combination of 2D Dual Tree Rotated Complex Wavelet Filters (RCWF) and 2D Dual Trace Complex wavelet Transform (CWT). This method provide features in 12directions against 3 and 6 directions in DWT and CWTrespectively. Iris features are obtained by computingenergies and standard deviation of detailed coefficientsubbands in 12 directions per stage, at 3 level ofdecomposition. Canbera distance is used for matching. This work is tested on UBIRIS database. It consists of 2400 iris images of 240 subjects which are captured in 02 distinct sessions i.e. 5 snaps of each subject per session. For each database total 500 enrolment attempts are performed and a total of 1600 genuine matching attempts and 3350 imposer matchingattempts. The experimental results improves the recognition rate and processing time as compared to wavelet transform based methods and Gabor wavelet based methods respectively. Natural shift invariance is the additional advantage of this scheme [10]. P. Yao et al. [11] presented an iris recognition algorithm based on modified Log-Gabor filters. The benefit of LogGabor filters in excess of complex Gabor filters is the past are strictly band pass filters and the latter are not. The property of strictly band pass makes the Log-Gabor filters more suitable to extract the iris phase features regardless of the background brightness. The performance is tested on CASIA database which consist of 756 images from 108 different irises. For each iris, 7 images were captured in 2 sessions. All possible comparisons are made between the iris images in the whole CASIA. Totally there are also 2, 268 intra-class comparisons and 283, 122 inter-class comparisons. Gabor filters have been successfully used in many applications; they are not perfectly suitable to encode the iris texture as the real parts of the filters are not strictly band pass. But result shows modified LogGabor filters can overcome the limitation of the complex 2D Gabor filters, use of modified Log-Gabor filters DC components will be included in the filters response, therefore more robust system performance can be achieved. Experimental results of this work have better recognition performance than the method using 2D Gabor filters. R. P. Wildes et al. [12] presented a system for persons verification founded on automated iris recognition. Main motivation behind that is human iris provides a particularly interesting structure on which to base a technology for noninvasive biometric measurement. This system is tested on 512 iris images. This system results in two forms. These results speak strongly in favor of using automated iris recognition as a method for biometric assessment. W. Boles, et al.[13] presented a human identification technique using images of the iris and wavelet transform. This algorithm specifically uses the zero crossings of the wavelet transform of the unique features obtained from the grey-level profiles of the iris and combination of translation, rotation and scale invariant process. He developed an algorithm for extracting unique features from images of the iris of the human eye and representing these features using the wavelet transform (WT) zero crossing. This representation is then utilized to recognize individuals from images of the irises of their eyes. This algorithm is tested using real images. Only the iris pattern of a single eye (left or right) was used to construct the representations in the database. The image size used was 128128, and the virtual circles used to collect data had a diameter of 45 pixels, where there were no reflections on the irises. As per results of algorithm it is clear that algorithm is insensitivity to variations in the lighting conditions and noise levels. performance of this work is compared with parameter called dissimilarity values and as per boles performance comparison shows that the dissimilarity values of the noisy for method M3 and method M4 at an SNR of 0 db are less than 23 D.Monro et al. [14] presented atechnique in the lead of differences in the power spectrum of fragments from normalized iris images and verified with the set of 2174 images from 308 eyes and tuned greater than a range of parameters. For identity recognition with weighted Hamming Distance metric 100 S. Rakshit et al. [17] described flexibility of identity verifi- cation systems to sub-sampling and compression of human iris images is implemented for three high performance algorithms and for the verification of same 2156 images from 308 eyes are mapped into a rectangular format with 512 pixels circumferentially and 80 radials. For identity verification of person the 48 rows adjacent the pupils were in use and the images were sub-sampled by Fourier domain processing and Fourier coefficients are required circumferentially and 16 radials to preserve 99.99the verification algorithms. Insignificant humiliation in proof is observed 171 circumferential and 16 radial Fourier coefficients are preserved with corresponding sampling at 342 by 32 pixels. In the midst of firmness by JPEG 2000, improved routine is observed down to 0.3 BPP qualified to noise reduction exclusive of significant loss of texture. To verify that no algorithm is degraded, it is recommended that normalized iris images should be exchanged at 512 x 80 pixel resolutions, compressed by JPEG 2000 to 0.5 BPP. S. Majumder et al. [18] presented SVD and error control coding based digital image watermarking. Individual use of SVD in watermarking incorporates errors, by a zigzag scan operation on pixels done before coding, increases the robustness. Hence author proposed use of both in single algorithm and implemented algorithm later applied and tested on the standard checkmark techniques practically by attacking the watermark image against against standard simulated attacks and recovering the watermarked logo from it. With the standard Checkmark 1.2 attacks Encoding and detection method has been simulated, for the Logo application and approximately 96 S. Majumder et al. [19] presented iris biometric watermarking based on SVD and wavelet. The algorithm here for the biometric generation has been kept very simple using Singular value decomposition and wavelet transform to reduce complexity of implementation. The database of eye images obtained from university of bath is taken. There are 20 images of each eye (both left and right) of 20 different persons. Thus they have a database of 2 20 20 images of which only the left eye images are taken, that is, 400 images. Moreover the integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. Thus this scheme provides a secure robust-imperceptible watermarking technology in total. D. Mathivadhani et al. [20] presented a technique using wavelet decomposition and Visual Cryptography. For biomet ric authentication 1D wavelet decomposition is used decompose the images. This algorithm is tested over with three cover images namely, Lena, Baboon and Pepper, one iris image and one secret image. The experimental result of this work showed that the planned scheme can resist various attacks while maintaining the visual quality of the cover image, During experimentation it was found that the size of the biometric should be less 40 S. Priyalakshmi et al. [21] presented robust and secure image authentication system by watermarking and iris biometric. The data is powerless in opposition to unapproved right to use and capture. To overcome this problem this paper presented a simple and efficient method of consolidating watermarking and biometrics for embedding and authentication of sensitive images. This method provides a secure way that first represents host image in critical band representation by applying DWT (Discrete wavelet Transformation). The SVD (Singular Value Decomposition) is adopted here to obtain a set of matrices and then embedding the secret message with the host image. Iris Biometric is chosen for the authentication of the Image. This method can be widely used in places which involves highly sensitive data. This method assures that the information will be accessed only by the authorized persons iris. F. Kolagar et al. [22] presented steganography of fingerprint images by using discrete wavelet transform. Definite functions that are similar in conditions of shape to Cos and Sin functions based on Fourier analysis. For two-dimensional images applying the discrete wavelet transform (DWT) is corresponding to the image processing in any dimension by two dimensional filters. The input image is divided by filter into four nonoverlapping sub-bands with multi-band HH, HL, LH and LL resolutions. Unacceptable results of steganography made by the wavelet transform caused to use the RDWT due to the low sampling, the changed form of image steganography and the undesired extraction of hidden image in the simulation stages. SVD to the LL sub-bands after applying RDWT to both front part and watermark image of the picture. Then single values of the front image corrected by using single values of watermark image. Resistance against common attacks is the main advantage of proposed system. Analysis and empirical results show the better performance of this work in comparison with other methods. D. WANG et al. [23] developed a watermarking scheme based on the singular value decomposition for biometric image is presented for remote users via insecure computer network. For verification of integrity of the received biometric image they marked good use of the singular values of SVD of biometric image. Other advantage of presented scheme is that it support any modification such as wavelet compression, JPEG compression, filtering, scaling, rotation, changing of pixel values and positions, cropping, sharpening, color reduction, line removal and using wrong key. And the biometric images quality is very high because only a few bits of authentication data are embedded. The system is tested on gray iris image of size 320280 as an original biometric image in the CASIA iris image database. Experimental results showed that the fragile watermarking scheme can be applied to the integrity authentication system based on biometric image. This work here by focuses implementation of a hybrid watermarking scheme using SVD and wavelet transform along with coded fingerprinting developed for protection of the intellectual property. Here wavelet transform plays the role of an efficient and robust tool due to its multi-resolution capability along with singular value decomposition (SVD) for watermarking. Both of these when implemented with coded fingerprinting not only resist collusion attacks but can also help tracing colluders. It does not require as a lot of basissignals as orthogonal intonation in organize to accommodate n number of users and can be used in conjunction with modulation to fingerprint gray scale image like multimedia sources. If this methodology is implemented for a larger matrix it can be wider in detection of colluders. M. Abdullah et al. [25] presented a method for defensive the honesty of the iris images using a demographic text as a watermark. The watermark text is embedded in the middle band frequency region of the iris image by interchanging three center band coefficients pairs of the Discrete Cosine Transform (DCT). Experimental results showed that exchanging more than one pair will make middle band scheme more robust against malicious attack along with making it resistant to image manipulation such as compression. The results also illustrate that our watermarking algorithm does not introduce discernible decrease on iris image quality or biometric recognition performance. III. CONCLUSION As per review of fragile and robust watermarking algorithms in this paper it is concluded that Watermarking empowers a security layer at the data level. Biometrics combined with watermarking is an added advantage to transmit a sensitive data over the internet and if DWT combined with SVD gives better results without losing more information of the image when compared with DCT in watermarking. Also this method can be used for applications which are less tolerant to degradation. Conjoining Biometrics with Watermarking is an added advantage. Hence this method can be used to transmit sensitive data such as medical images, military secrets, etc.

REFERENCES

[1]. D. Khannah and Dr. gobi, survey on biometric based digital watermarking technique and applications, Global journal of computer science and technology, vol. 13, issue. 8, pp. 22-27, 2013.

[2]. Rimmi K Patel, A Review on Watermarking Techniques for Biometric Security, IJARESM, pp. 1-6, 2012.

[3]. C.Karthikeyan and D.Selvamani , Multimodal Biometric Watermarking Techniques: A Review, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 10, pp. 12542-12546, October 2014.

[4]. S.Sanderson and J.H.Erbetta, Authentication for Secure Environments Based on Iris Scanning Technology, pp. 1-8. 2009.

[5]. Richard P. Wildes, Iris Recognition: An Emerging Biometric Technology, proceedings of the IEEE, VOL. 85, NO. 9, pp. 1348-1363, September 1997.

[6]. Ion Marqus, Manuel Graa, Image security and biometrics: A review, Grupo de InteligenciaComputacional, UPV/EHU www.ehu.es/ccwintco

[7]. Ruizhen Liu and TieniuTan,An SVD-Based Watermarking Scheme for Protecting Rightful Ownership, IEEE Transactions on Multimedia, Vol. 4, No. 1, March 2002, pp. 121-128

[8]. Stephane G. Mallat, A Theory For Multiresolution Signal Decomposition: The Wavelet Representation, Ieee Transactions On Pattern Analysis And Machine Intelligence. Vol I I . No. 7. July 1989. Pp. 674-693. 5

[9]. Rajesh M. Bodade, Dr. Sanjay N. Talbar, Iris Recognition Using Rotational Complex Wavelet Filters: A Novel Approach, 2008 IEEE, 658-686.

[10]. N.G. Kingsbury, The dual-tree complex wavelet transform: A new technique for shift invariance and directional filters, Proc. 8th IEEE DSP Workshop, Utah, Aug. 912, 1998, paper no. 86-20.

[11]. Peng Yao, Jun Li, Xueyi Ye, Zhenquan Zhuang, Bin Li, Iris Recognition Algorithm Using Modified Log-Gabor Filters, The 18th International Conference on Pattern Recognition (ICPR06), computer society, IEEE, 2006.

[12]. R. P. Wildes J. C. Asmuth G. L. Green S. C. Hsu R. J. Kolczynski J. R. Matey S. E. McBride, A System for Automated Iris Recognition, 1994 IEEE, pages 121-128

[13]. W. W. Boles and B. Boashash. A Human Identification Technique Using Images of the Iris and Wavelet Transform , IEEE transactions on signal processing, vol. 46, no. 4, pages no- 185-198, April 1998

[14]. D. M. Monro and D. Zhang ,Effective Human Iris Code with Low Com-plexity, Department of Electronic and Electrical Engineering, University of Bath, BA2 7AU, UK, 2005 IEEE.

[15]. J. Daugman, High Confidence Visual Recognition of Persons by a Test of Statistical Independence, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 15, No. 11, PP. 1148-1161, 1993

[16]. L. Ma, T. Tan, etc,Efficient Iris Recognition by Characterizing Key Local Variations, IEEE Trans. on Image Processing, Vol. 13, PP. 739-750, 2004.

[17]. S. Rakshit and D. M. Monro, An Effect of Sampling and Compression On Human Iris Verification , ICASSP 2006 , IEEE , pp 237-340.

[18]. S. Majumder, T. S. Das, V. H. Mankar and S. K. Sarkar, SVD and Error Control Coding based Digital Image Watermarking, International Conference on Advances in Computing, Control, and Telecommunication Technologies, computr society, IEEE, 2009, pp. 60-63.

[19]. Swanirbhar Majumder, Kharibam Jilenkumari Devi and Subir Kumar Sarkar, Singular value decomposition and wavelet-based iris biometric watermarking, The Institution of Engineering and Technology 2013, Vol. 2, Iss. 1, pp. 2127.

[20]. Mrs. D. Mathivadhani, Dr. C. Meena, Biometric Based Authentication Us-ing Wavelets and Visual Cryptography , IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, IEEE, pp 291-295.

[21]. S. Priyalakshmi and Sumathy Eswaran, Robust and Secured Image Authentication System by Watermarking and Iris Biometric, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015, pp. 32-36.

[22]. Farinaz Dehestani Kolagar and Seyed Mohammad Jalal Rastegar Fatemi, Steganography Of Fingerprint Images By Using Discrete Wavelet Transform, Volume-4 Issue- 3, pp. 367-376, 2015.

[23]. De-song WANG, Jian-ping LI and Xiao-yang WEN, Biometric Image Integrity Authentication Based on SVD and Fragile Watermarking, Congress on Image and Signal Processing, computer society, IEEE, pp. 679-608, 2008.

[24]. M. Saikia, S. Majumder, T. S. Das, Md. A. Hussain and S. K. Sarkar, Coded Fingerprinting based Watermarking to Resist Collusion Attacks and Trace Colluders, International Conference on Advances in Computer Engineering, Computer society, IEEE, pp. 120-124, 2010.

[25]. Abdullah MAM, Dlay SS, Woo WL. Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform. In: 10th International Conference on Computer Vision Theory and Applications (VISAPP 2015). 2015, Berlin, Germany: INSTICC.