RESEARCH ARTICLE OPEN ACCESS

A SURVEY ON NOVEL AND ROBUST MEDICAL WATERMARKING SCHEMES

K.Meghana Reddy[1], K.Swaraja[2]
1(Assistant Professor, Dept. Of ECE, AITS, Kadapa, AP,)
2(Professor, Dept. Of ECE, GRIET, Hyderabad, Telangana,)

Abstract:

In this paper a brief conversation on survey of dissimilar features of novel and robust digital image watermarking schemes are focused. The present survey includes the broad concepts such as major features of digital watermark, different categories of watermarking schemes, various evaluation parameters for digital watermarking schemes along with the recent state-of-art watermarking techniques. Further, this survey will influence the researchers towards the development of robust and secure watermarking schemes to safeguard integrity and confidentiality of patient's critical medical data, counter to unauthorized access besides securing e governance applications.

***Keywords*—Spatial and transform domain schemes, Medical Image watermarking, Imperceptibility, Robustness and Payload.**

I. INTRODUCTION

The new advancements in high-bandwidth digital communication technologies haveallowed newer opportunities of transmitting large volume of multimedia datathrough the internet [1, 2] that coves rural/remote areas, accident sites, ambulance, and hospitals [3]. The transmission of medical data over an open communication channel poses different possibilities of threat that severely affect its authenticity, integrity, and confidentiality which demands for implementing some kind of digital watermarking schemes to avoid ready attention and preventing access by an unintended recipient.Thus it should be protected from unauthorized users by implementing some mechanisms. Investigators are utilizing watermarking schemes for the shielding of these media contents from unauthorized users.In this technique, some type of watermarks (digital data) areinserted within the test multimedia contents for the persistence of annotation, copyright, content authentications of the digital media in severalchallenging applications.The other applications include electronic governance, real time video/ audio delivery, electronic advertising, digital library and web publishing healthcare, forensics, finger printing and many more.Despite the above applications,the bandwidth during the transmission of large media files is reduced using this scheme. E-governance is a communication based technologies to offer a way of appropriate access of government information and facilities [1]. However, information safety is the crucial issue for a regimented e-Government system.Currently,watermarking scheme affords a value added tools in the area of electronic governance to safeguard as well as to notice the illicitpractice of digital information.Despite broad literature on various application fields, a very limited work has been implemented towards the exploitation of health-oriented perspectives of watermarking [4, 5, 6-8]. The watermarking schemes in the areas of telemedicine entail extreme care when inserting additional data within the images since the additional information should not disturb the qualityof image. The confidentiality, reliability and accessibility are significant security necessities with electronic patient record (EPR) data interchange through unsecured channels [3, 5, 9].

The rest of the paper is structured as follows. The various categories of digital watermarking schemes are provided in Section 2. Section 3 offers

major features of digital watermark and evaluation parameters for digital watermarkingareincluded in section4. Various recent state-of-the-art watermarking techniques and distinct watermarking methods introduced in the preceding years are reported in Section 5. Subsequent to this conclusion of the paper is presented in section 6.

II. DIFFERENT CATEGORIES OF WATERMARKING SCHEMES

Watermarking schemes are classified briefly as shown in Fig. 1. According to the nature of document, With reference to this figure, watermark is identified as four dissimilarkindssuch as text, image, audio and video. Further, on the basis of human recognizing, it is alienated into invisible and visible watermark. From theinvestigationobtainable, the invisible watermark possibly will be robust and fragile. Robust watermarking could be private, public invertible, noninvertible, quasi invertible, non-quasi invertible. Yet, the fragile watermark is unnoticeable. Many researchers are utilizing the amalgamation of robust and fragile watermark in a similar media document to make it further secure. Instead a semi-fragile watermark defines a watermark that is modest by authentic alterations, but uncertain by illegal alterations. Domain based watermarking is classified into spatial and frequency/transform domain schemes. In the spatial domain schemes, the pixel value, bit stream or code value is operated and data is encoded directly. Moreover, this scheme is computationally simple. However, transform domain schemes are computationally complex and robust for signal processing attacks [10]. For the robust and imperceptible watermarking schemes, the transform domain schemes are upright choice. Essential domain based schemes are presented in Fig. 3 [10,11, 12].

Currently, maximum of potential researchers are exploiting blind, semi-blind, non-blind, robust, fragile and semi-fragile watermarking schemes for numerousgrowing applications. Certain watermarking schemes are apt for precise applications, while the others are not well identified yet but are highly capable.

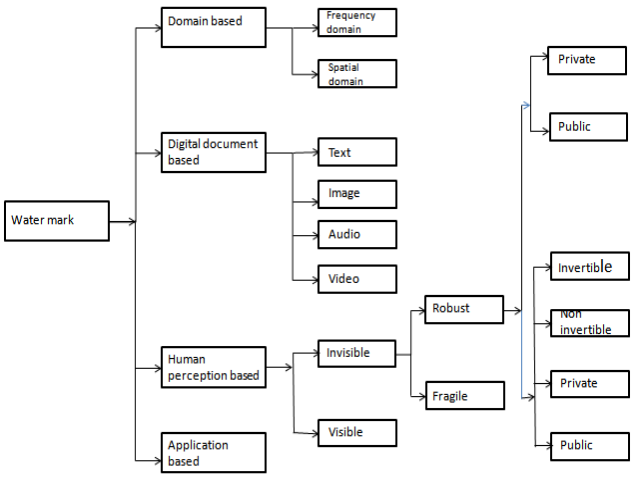

Fig 1: Types of watermarking techniques

III. MAJOR FEATURES OF DIGITAL WATERMARK

The significantfeatures of digital watermark are labeled in Fig. 2 [12]. These features are very essential for general watermarking systems.It is welldefined as follows: Robustness is opposition of digital watermark to selected class of transformations. Safety of watermark is aneffort to eliminate or amend it without damaging test image. Data payload is the overall information that it comprises. Imperceptibility is a measure of perceptual clearness of the watermark. Fragile watermark object is to provide content authentication, this is reverse of robustness.

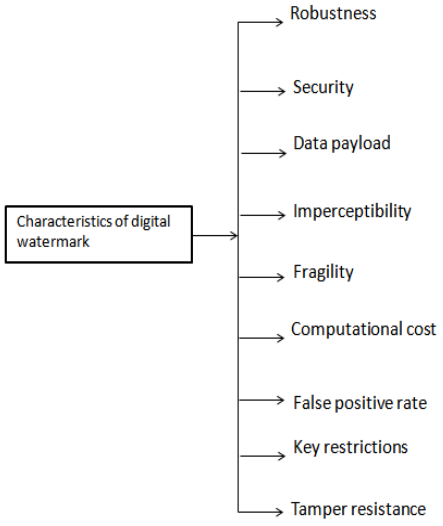

Fig 2: Characteristics of Digital watermark

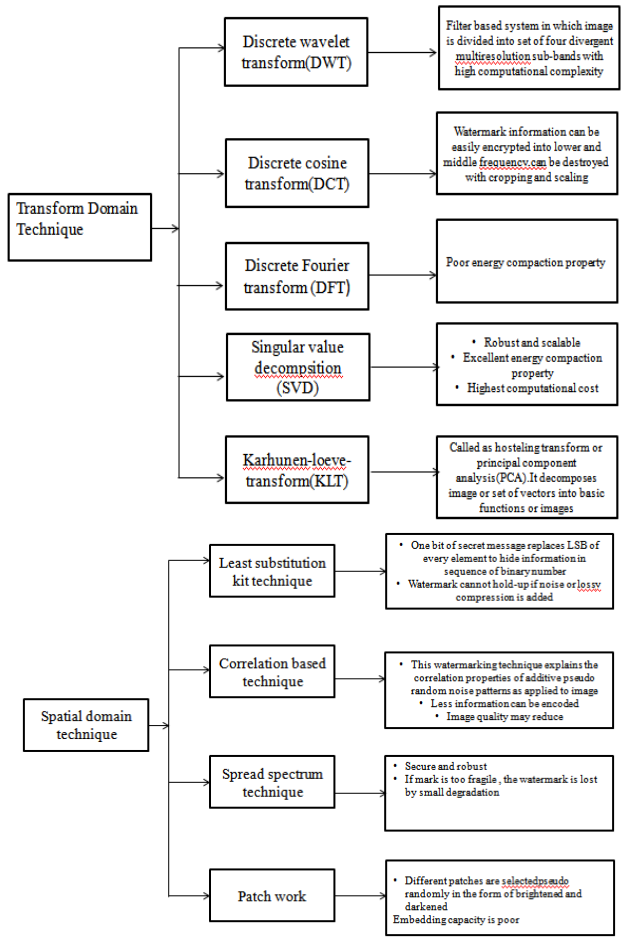

Fig 3:Spatial domain and transform domain Schemes

IV. EVALUATION PARAMETERS FOR DIGITAL WATERMARKING

The performance criteria for watermarking in any case must comprise perceptual transparency, robustness, capacity, and security. The entire simulation results are evaluated by finding the Imperceptibility, Robustness and Data payload.

A. Imperceptibility

Imperceptibility is a quality of the watermarked video. It must not change even after inserting the watermark into the image, video or text, and the watermark ought to be perceptually indiscernible. The visual quality of the watermarked video is estimated by the PSNR (peak signal-to-noise ratio). PSNR is a commonly used objective perceptual quality measure. The discrepancy of the watermarked andattacked frames from the original video frames is determined by calculating the PSNR and is delineated by Eq (1).

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad (1)$$

To evaluate the PSNR, the earliest Mean Square Error (MSE) between the original and watermarked frame is computed, as MSE is the mean square error connecting the original video and the watermarked video which is given by Eq (2).

$$MSE = \frac{1}{R\times C}\sum_{i}^{R}\sum_{j}^{C}[V(i,j) - V'(i,j)]^2 \qquad (2)$$

At this moment, the notations Rand Ccorrespond to the width and height of a frame, V(i, j)is the pixel value of coordinate (i, j)in original video, and V'(i, j)is the pixel value of the watermarked video. Thus the invisibility is measured by calculating the average mean square error (MSE) and the average PSNR. The higher the PSNR, the better is the quality of the video. In general, for digital images, noise with PSNR is higher than 30 dB which is hardly noticeable.

B. Robustness

It is the capability of a detector to extort the unseen watermark from some distorted watermarked data. It is frequently assessed through the endurance of a watermark after attacks, such as, compression, re-sampling, cropping, geometric distortions, frame swapping, frame dropping, frame averaging and scaling. Robustness is the resistivity of the watermark in opposition to common signal processing and malicious attacks. It is supposed to be skilled in extorting the watermark from the watermarked video. Even if the algorithmic principle of the watermarking method is public, the watermark should not be viable to be taken away. For comparing the similarities between the original and extracted watermarks, the two-dimensional normalized correlation (NC) value was employed. The NC value can be between '0' and '1'. In principle, if the NC value is closer to '1', the extracted watermark is getting more similar to the embedded one. In order to evaluate the performance

of watermarking algorithm objectively, NC (normalized correlation) function is evaluated and computed by using Eq. (3)

$$NC(V,V') = \frac{\sum_{i=1}^{R}\sum_{j=1}^{C}[V(i,j).V'(i,j)]}{\sum_{i=1}^{R}\sum_{j=1}^{C}[V(i,j)]^2} \quad (3)$$

Where, V' is the extracted watermark and V is the original watermark. V (i,j) represents original watermark image and V'(i,j) represents the extracted watermark image.

C. Payload

It is the quantity of information which is interleaved into original video (i.e. mark size). We delineate the watermark cost 'δ' as the augment in number of bits utilized to encode the watermarked video for every watermark bit and is given by Eq (4). Where $TB_{original}$is the number of bits utilized to code the original video sequence, $TB_{watermarked}$ is the number of bits exploited to code the watermarked video sequence and $N_w(f)$ is the overall number of watermarked coefficients in that video sequence.

$$\delta = \frac{TB_{watermarked} - TB_{original}}{\sum_{f=1}^{L_f} N_w(f)} \quad (4)$$

V. LITERATURE SURVEY

An adaptive image watermarking schemecentered on DCT-SVD aimed at e-government text is presented in [1]. The watermark content is inserted into the singular values of DCT transformed test image by genetic algorithm (GA). The scheme is strong and indiscernible for diverse attacks. Amini et al. [13] planned a blind watermark decoder in DWT domain by exploiting vector based Hidden markov model (HMM). The simulation outcomesspecified that the scheme is extremelystrong for numerous attacks comprising checkmark and presentedpoor bit error rate than other state-of-the-art techniques [14, 15]. Moreover, the scheme is also appropriate for the color images. Conversely, poor directional information besidesdeficiencyin shift sensitivity is chiefconfines of the DWT centered watermarking schemes. Ghazvini et al. [16] established ageneric algorithm based robust watermarking practicebymerging DWT and DCT. The watermark data is encoded by two random sequences pattern then the encoded data areinserted into the chosen sub-bands of the DWT test image. Outcomesspecified that the scheme presentedimproved Peak signal-to-noise ratio (PSNR) in additionto the normalized correlation (NC) when compared toformer high-quality methods [17,18,19]. Still, the scheme is computationally eliterather thanemployingDWTor DCT independently. Singh et al. [20] projected a semi-blind watermarking algorithmby amalgamating non-sub-sampled contourlet transform (NSCT), redundant discrete wavelet transform (RDWT) besides SVD. In this algorithm, improved reconstructionof the watermarked image is attained through NSCT and RDWT. Additionally, robustness as well as security of the watermark is accomplished through SVD and Arnold transform. During Simulation, the schemepresentedamended performance in terms of PSNR,Correlation coefficient (CC), Structural similarity index metric (SSIM) besides bit error rate (BER) than other prevailingschemes [21,22,23]. Though, redundant wavelet transforms centered watermarking schemes are computationally elite. Lei et al. [24] projected an intelligent multiple watermarkingmethodutilizing integer discrete wavelet transform (IDWT) and SVD.

Two dissimilar watermarks are scrambled into carefully chosen IDWT sub-bands of the test image for the persistence of copyright safety and contentauthentication. Moreover, authors have established an artificial bee colony (ABC) algorithm forfinest parameter assortment to achieve a virtuous trade-off among the foremost performance constraints of watermarking scheme. Simulation results revealed the benefit of projectedscheme as associated to other state-of-the-art schemes[25]. Further, the scheme is also active to struggle brute-force attack. To progress the safety of watermark, investigators areexploiting theamalgamation of watermarking besides encryption practices. Still, outmoded encryptionapproaches such as Advanced Encryption Standard (AES), Data Encryption Standard (DES)and Rivest, Shamir, and Adleman (RSA) are very deliberate and not appropriate for extremely real timemultimedia files [26].

Ansari and Pant [6] developed a watermarking algorithm byrelating spatial and transform domain schemes. During theprocedure of inserting the watermark, the DWT is applied on carefully chosentest image and robust watermark image. The singular value of the test imageis amended with the principal components of the watermark image. In [27] a blind watermarking scheme utilizingcolor images for the persistence of copyright security and image authentication is accessible.The 'Y' component of the color model is decomposed initially by DWT,in addition the low frequency components of the DWT test image is quantized by luminance quantization table. Next, the watermarklogo is inserted into the high frequency component of the 'Y' DWT test imageby exploiting the outcome of the frequency components quantization of the test image. The performance of the scheme is evaluated in termsof PSNR, SSIM and exact rate. The simulation outcomespresentedenhanced performance associated to the other state-of-the-art methods [28,29,30].

VI. CONCLUSION

In this paper, a brief introduction to the digital image watermarking schemes and the chieffeatures of digital watermarkis specifiedas well as dissimilarcategories of watermarking schemeswere discussed andvarious evaluation constraints of digital watermarking schemeswere listed. Further, the paper presented the summary of numerous state-of-the-art watermarking schemes. This exploration will also help the investigators to progressthesafety, robustness and confidentiality of the watermarking system to secure e-governance applications.

REFERENCES

1. Horng SJ, Rosiyadi D, Fan P, Wang X, Khan MK (2013) An adaptive watermarking scheme for e-government document images. Multimed Tool Appl 72(3):3085–3103 35.
2. Sharma A, Singh AK, Kumar P (2017) Combining Haar wavelet and KarhunenLoeve transforms for robust and imperceptible data hiding using digital images.JIntell Syst. https://doi.org/10.1515/jisys-2017-0032.
3. Abbas NH, Ahmad SMS, Ramli ARB, Parveen S (2016)A multi-purpose watermarking scheme based on hybrid of lifting wavelet transform and Arnold transform.International conferenceon multidisciplinary in IT and communication science and applications.
4. K.Swaraja (2017) A Hybrid Secure watermarking technique in Telemedicine, International Journal of Engineering and Technology (IJET), 9(3), ISSN: 2319-8613.
5. Ali M, Ahn CW, Pant M (2017) An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional Fourier transforms. Multimed Tool Appl 1–23.
6. Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern RecognLett 94:228–236.
7. K.Swaraja (2017) Blind Hybrid watermarking for Security of Medical Images, IEEE Conference on I2C2-2017, June 23-24, Coimbatore, India.
8. K.Swaraja (2017) A Secure Hybrid watermarking technique in Medicine for Medical Images, ICMTES, Andhra Pradesh, India, June 2-3.
9. Bas P, Chassery JM, Macq B (2002) Geometrically invariant watermarking using feature points. IEEE Transaction Using Image Processing 11(9):1014–1028.
10. Mohanty SP, SenguptaA, Guturu P, Kougianos E (2017) Everything youwant to know about watermarking: from paper marks to hardware protection: from paper marks to hardware protection. IEEE. Consumer ElectronicsMagazine 6(3):83–91
11. Singh AK, Dave M, Mohan A (2014) Wavelet based image watermarking: futuristic Conceptsin information security. ProcNatlAcadSci, India, Sect A 84(3):345–35.
12. Mingzhi C, Yan L, Yajian Z, Min L (2013) A combined DWT and DCT watermarkingscheme optimized using genetic algorithm. J Multimed 8(3):299–305.
13. AminiM, Ahmad MO, Swamy MNS (2017) Digital watermark extraction in wavelet domain using hidden Markov model. Multimed Tool Appl 76(3):3731–3749.
14. Kalantari NK, Ahadi SM (2010) A logarithmic quantization index modulation for perceptually better data hiding. IEEE Trans Image Process 19(6):1504–1517.

15. Mingzhi C, Yan L, Yajian Z, Min L (2013) A combined DWT and DCT watermarkingscheme optimized using genetic algorithm. J Multimed 8(3):299–305.

16. Ghazvini M, Hachrood EM, Mirzadi M (2017) An improved image watermarking method in frequency domain 12(2):260–275.

17. Mingzhi C, Yan L, Yajian Z, Min L (2013) A combined DWT and DCT watermarkingscheme optimized using genetic algorithm. J Multimed 8(3):299–305Consumer Electronics Magazine 6(3):83–91.

18. Wang SH, Lin YP (2004) Wavelet tree quantization for copyright protection watermarking. IEEE TransImage Process 13(2):154–165.

19. Yuan Y, Huang D, Liu D (2006) An integer wavelet basedmultiple logo-watermarking scheme. Computerand Computational Sciences, First International Multi-Symposiums on Computer and Computational Sciences, Hanzhou 2:175–179.

20. Singh S, Rathore VS, Singh R, Singh MK (2017) Hybrid semi-blind image watermarking in redundantwavelet domain. Multimed Tool Appl 76(18):19113–19137ational Sciences, Hanzhou 2:175–179.

21. Rosiyadi D, Horng SJ, Fan P, Wang X, Khan MK, Pan Y (2012) Copyright protection for e-government document images. IEEE Multimedia 19(3):62–73.

22. Singh S, Rathore VS, Singh R (2017) Hybrid NSCT domain multiple watermarking for medical images.Multimed Tool Appl 76(3):3557–3575.

23. Srivastava A, Saxena P (2013) DWT-DCT-SVD based semi-blind image watermarking using middle frequency band. IOSR Journal of Computer Engineering 12(2):63–66.

24. Lei B, Zhao X, Lei H, Ni D, Siping C, Zhou F, Wang T (2017) Multipurpose watermarking scheme via intelligent method and chaotic map. Multimed Tools Appl.1–23.

25. Zhang L, Gao Y, Xia Y, Dai Q, Li X (2015) A fine-grained image categorization system by Celletencodedspatialpyramid modeling. IEEE Trans Ind Electron 62(1):564–571.

26. Cao X, Fu Z, Sun X (2016) A privacy-preserving outsourcing data storage scheme with fragiledigitalwatermarking-based data auditing. J ElectrComputEng 2016(2016):1–7.

27. Liu XL, Lin CC (2016) Blind dual watermarking for color images' authentication and copyright protection.IEEE Trans Circuits Syst Video Technol.

28. K.Swaraja (2017) Watermarking patient record in Medical Images with M-ary Modulation, ICSTSD, Hyderabad, India, April 8.

29. K.Swaraja (2017) Protection of Medical Image Watermarking, Journal of Advanced Research in Dynamical and Control Systems (JARDCS), Special Issue 11, ISSN: 1943-023X.

30. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and genetic algorithm. PatternRecognLett 34(3):671–683.