BLIND DUAL WATERMARKING FOR COLOR IMAGES USING DOUBLE KEY AUTHENTICATION

[1]K.DURGA GANGA RAO, [2]T.RAVINDRA

[1]Assistant Professor, [2]M.Tech Student

DEPARTMENT OF ECE

Jawaharlal Nehru Technological University (Autonomous), Kakinada.

Abstract—This paper presents a blind dual watermarking mechanism for digital color images in which invisible robust watermarks are embedded for copyright protection and fragile watermarks are embedded for image authentication. For the purpose of copyright protection, the first watermark is embedded using the discrete wavelet transform in YCbCr color space, and it can be extracted blindly without access to the host image. However, fragile watermarking is based on an improved least significant bits replacement approach in RGB components for image authentication. The authenticity and integrity of a suspicious image can be verified blindly without the host image and the original watermark. The combination of robust and fragile water-marking makes the proposed mechanism suitable for protecting valuable original images. The experimental results indicated that the proposed watermarking mechanism can withstand various processing attacks and accurately locate the tampered area of an image. With an digital watermark scheme is proposed to protect the copy right of network digital image. In this different types of water marks attacks by analysing the attack principle, a double key water mark embeddeding and extracting scheme is proposed to display encryption and decryption images for further safetyness of an watermarked image during transmission and reception process.

Keyword: Digital watermarking, Authentication, copyright protection, discrete wavelet transform (DWT), least significant bit (LSB), watermarking.

I. INTRODUCTION

The quick advancement of a data arranged society, progressively huge amounts of digitalized material are being transmitted over the Internet. Concerns relating to the upgrade of security and assurance against infringement of computerized pictures have turned out to be basic over the previous decade. Computerized watermarking [1]–[6] is presently a moderately engaged method went for giving a dependable method to confirm pictures or secure copyright assurance; in this strategy, a watermark is normally inserted imperceptibly in the advanced picture to abstain from pulling in the consideration of vindictive aggressors. As per the ideal heartiness of the implanted watermark, computerized watermarking systems are separated into powerful watermarking [4]–[6] and delicate watermarking [1]–[3]. The fundamental motivation behind vigorous watermarking method is frequently to ensure the responsibility for pictures, while the delicate watermarking procedure is utilized to validate the uprightness of pictures

Hearty watermarking is regularly utilized for copyright insurance ,and in this manner it is intended to oppose assaults that endeavor to evacuate or wreck the watermark without essentially corrupting the visual nature of the watermarked picture. In vigorous watermarking, unquestionable watermarks of clients, for example, logos or copyright data, are inserted into the host pictures. Afterward, the verifiers can extricate the watermarks and affirm proprietorship through the watermarked pictures. Vigor is one of the significant purposes of concern, which implies that the removed watermark must be strong enough for the responsibility for host picture to be checked even after the watermarked picture has been exposed to flag preparing assaults. Notwithstanding, for expanding the strength of a watermarked picture, past strong watermarking procedures frequently change huge regions of the host picture, which can cause genuine mutilation of the nature of the watermarked picture. This mutilation may enable malevolent aggressors to distinguish which information are profitable, enabling them to perform cryptanalysis and get the secret information. Along these lines, it is as yet a notable issue in the watermarking field to build up a powerful watermarking plan that can convey exceptional heartiness while keeping up great visual nature of watermarked pictures. Then again, delicate watermarking was grown especially for picture confirmation, in which the inserted watermark ought to be delicate with the goal that any alterations of the pictures will be evident. The validness of the picture ought to be checked completely if the watermarked picture has been controlled in any capacity, for example, JPEG pressure, collection, or editing. Since the less huge zones of the host picture are

modified in delicate watermarking, the visual nature of a delicate watermarked picture is typically superior to that of the powerful watermarked picture. The precision of the confirmation is the significant worry in delicate watermarking, and systems that were created before 2000 concentrated primarily on identifying whether a picture had been messed with or not. In any case, they didn't unmistakably determine where the picture had been adjusted. In the course of the most recent 15 years, a few picture validation plans have been created to find the altered zones, however the ability of doing as such is scarcely palatable, and only one out of every odd changed pixel is destined to be distinguished effectively. Moreover, the majority of the delicate watermarking plans are non visually impaired, and unique watermark data is required during the check methodology.

To fulfill the basics of hearty and delicate watermarking plans clarified above, in this paper, we present a visually impaired double watermarking system for shading pictures. An undetectable and strong watermark is installed for copyright security, and an imperceptible and delicate watermark is inserted for picture confirmation in the meantime in our plan. The discrete wavelet change (DWT) in the Y channel of the YCbCr shading space is utilized for powerful watermarking. After one dimension of DWT disintegration, the low–low (LL) sub band of Y is quantized by the luminance quantization table. The strong watermark is inserted in the high–high (HH) sub-band by expertly supplanting it with the aftereffect of the LL quantization. What's more, the delicate watermark for picture verification is installed freely on each RGB shading channel as per an improved least noteworthy piece (LSB) substitution approach [10]. The copyright and validness of watermarked picture can be confirmed indiscriminately without the host picture. The reenactment results demonstrated that the proposed double watermarking component can withstand different preparing assaults and find the altered zone of the picture precisely. Besides, the proposed instrument gives watermarked picture wonderful visual quality, which makes it appropriate for ensuring important unique pictures.

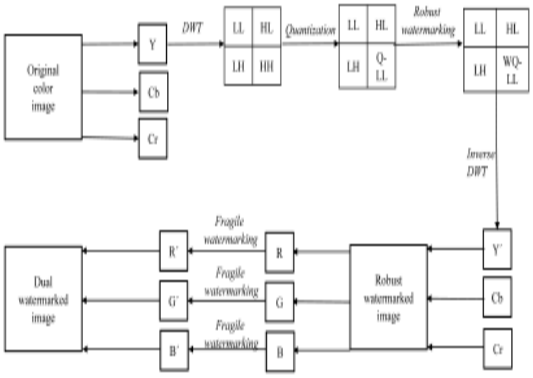

Fig. 1.Our watermark embedding procedure.

II. LITERATURE SURVEY

An adaptive image watermarking scheme centered on DCT-SVD aimed at 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 practice by merging DWT and DCT. The watermark data is encoded by two random sequences pattern then the encoded data are inserted into the chosen sub-bands of the DWT test image. Outcomesspecified that the scheme presentedimproved Peak signal-to-noise ratio (PSNR) in addition to the normalized correlation (NC) when compared toformer highquality methods [17,18,19]. Still, the scheme is computationally elite rather than employing DWT or DCT independently. Singh et al. [20] projected a semi-blind watermarking algorithm by 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 bruteforce attack. To progress the safety of watermark, investigators are exploiting the amalgamation 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

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 chosen test 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

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 an effort 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.

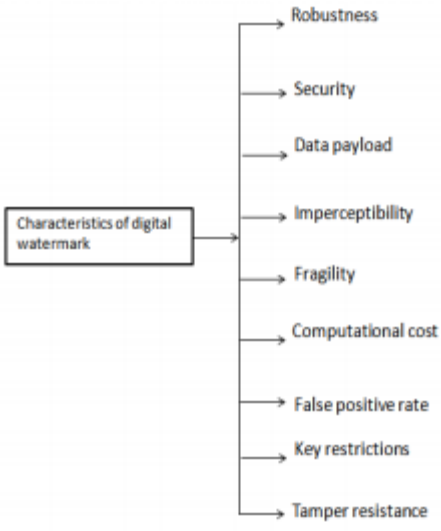

Fig 2: Characteristics of Digital watermark

MULTIPLE WATERMARKING TECHNIQUES

In multiple watermarking techniques multiple watermarks are embedded into the original image. The works in the literature related to multiple image watermarking techniques are discussed below. A wavelet-based watermarking scheme to embed multiple watermarks in medical images is proposed in [25]. Their scheme offers medical confidentiality and record integrity, the quality of watermarked images to achieve higher PSNR values. An wavelet based watermarking algorithm the watermarks are embedded in different sub-bands with variable scaling factor [26]. The scaling factor is high for the LL sub-band and it is low for other three sub-bands. A multiple watermarking technique by adopting integer wavelet transform is presented in [27]. Their method is robust to a wide variety of attacks. MahaSharkas et al. [28] tested a novel image watermarking technique in the wavelet domain. Their method achieves more security and robustness. A multiple watermarking techniques for color images in spatial domain are proposed in [29]. A novel multiple watermarking algorithm which embedded two watermarks into original image in different frequency by using bandelet transform is proposed in [29]. Their watermarking algorithm has a good performance in invisibility and robustness. An image watermarking technique is proposed in [31], to embed multiple binary watermarks into original images based on the concept of Visual Cryptography. VijendraRai et al. [32] presented a multiple image watermarking based on dither quantization. Their algorithm is superior in terms of embedding capacity and attacks. A multiple robust digital watermarking system for still images is proposed in [33]. Their method shows the results are resistant to different types of attacks. A review of multiple watermarking for text documents is presented [34]. Their multiple watermarking approach increases the security and robustness.

Successive watermarking

In successive watermarking technique, the multiple watermarks are embedded one after the other, from the watermarked images the multiple watermarks are extracted from one after other. This approach is also called Rewatermarking technique. The three main categories of multiple watermarking techniques are distinguished in [35]. The use of classical single watermarking scheme in a multiple re-watermarking scenario is discussed in [36]. Comparison of blind and non-blind algorithms is focused in their method

Segmented watermarking

In segmented watermarking technique, the original image is separated into different segments and each watermark is embedded into its specific share. Wheeler et al. [37] proposed weighted segmented watermarking of still images in which

segments are formed by dividing the image into square blocks, each of which contains one contributor's watermark. NanthaPriya et al. [38] proposed the segmented image is modeled as mixture generalized Gaussian distribution and their model is the basis of mathematical analysis of various aspects of the watermarking process such as probability of error and embedding strength adjustment

Composite watermarking

In composite watermarking, multiple watermarks are combined into a single watermark which is subsequently embedded in one single embedding step. Mina Deng et al [39] proposed a buyer seller watermarking protocol based on composite signal representation in the encrypted domain. Their proposed composite embedding can be performed in the encrypted domain by simply using an additively homomorphic cryptosystem.

IV. CONCLUSION

In this paper, we presented a blind dual watermarking mechanismfor color the authentication of images and copyrightprotection. The invisible, fragile, and robust watermarks areembedded into the spatial domain of the RGB color spaceand into the frequency domain of the YCbCr color space.The major contribution of this paper is that our mechanismcan achieve copyright protection and image authenticationsimultaneously, and the extraction of watermarks from theprotected image can be processed blindly without the originalhost image and watermarks. According to the experimentalresults, the proposed watermarking mechanism can withstandvarious processing attacks and locate the tampered area ofthe image accurately. Moreover, the dual watermarked imageis imperceptible, which makes the proposed mechanism suitablefor protecting valuable original images. Comparisonsof the functionality of our proposed mechanism with thefunctionalities of other well-known dual watermarking mechanismsclearly demonstrated the superiority of the proposedmechanism.

REFERENCES

[1] M. M. Yeung and F. Mintzer, "An invisible watermarking technique forimage verification," in *Proc. Int. Conf. Image Process.*, vol. 2. Oct. 1997,pp. 680–683.

[2] C.-C. Chang, Y.-P.Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognit.*, vol. 41, no. 10,pp. 3130–3137, 2008.

[3] A. K. Kamran and S. A. Malik, "A high capacity reversiblewatermarking approach for authenticating images: Exploiting downsampling,
histogram processing, and block selection," *Inf. Sci.*, vol. 256,pp. 162–183, Jan. 2014.

[4] W.-J. Chen, C.-C. Chang, and T. H. N. Le, "High payload steganographymechanism using hybrid edge detector," *Expert Syst. Appl.*, vol. 37,
pp. 3292–3301, Apr. 2010.

[5] Q. Su, Y. Niu, H. Zou, and X. Liu, "A blind dual color imageswatermarking based on singular value decomposition," *Appl. Math.*
Comput., vol. 219, no. 16, pp. 8455–8466, 2013.

[6] S. P. Maity, S. Maity, J. Sil, and C. Delpha, "Collusion resilientspread spectrum watermarking in M-band wavelets using GA-fuzzy
hybridization," *J. Syst. Softw.*, vol. 86, no. 1, pp. 47–59, 2013.

[7] C.-S. Lu and H. Y. M. Liao, "Multipurpose watermarking for imageauthentication and protection," *IEEE Trans. Image Process.*, vol. 10,
no. 10, pp. 1579–1592, Oct. 2001.

[8] P.-Y. Lin, J.-S.Lee, and C.-C. Chang, "Dual digital watermarking forInternet media based on hybrid strategies," *IEEE Trans. Circuits Syst.*
Video Technol., vol. 19, no. 8, pp. 1169–1177, Aug. 2009.

[9] F. Lusson, K. Bailey, M. Leeney, and K. Curran, "A novel approach todigital watermarking, exploiting colour spaces," *Signal Process.*, vol. 93,no. 5, pp. 1268–1294, 2013.

[10] C.-C. Lin, Y.-H.Chen, and C.-C. Chang, "LSB-based high-capacitydata embedding scheme for digital images," *Int. J. Innov.Comput., Inf.*
Control, vol. 5, no. 11, pp. 4283–4289, 2009

[11] *Information Technology-Digital Compression and Coding ofContinuous-Tone Still Images-Requirements and Guidelines*,
document CCITT Rec. T.81, Int. Telecommunication Union, 1992.

[12] L. Zhang, L. Zhang, X. Mou, and D. Zhang, "FSIM: A feature similarityindex for image quality assessment," *IEEE Trans. Image Process.*,
vol. 20, no. 8, pp. 2378–2386, Aug. 2011.

[13] R.-Z. Wang, C.-F.Lin, and J.-C. Lin, "Image hiding by optimal LSBsubstitution and genetic algorithm," *Pattern Recognit.*, vol. 34, no. 3,
pp. 671–683, 2001.

[14] 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.