European Journal of Applied Sciences 8 (4): 230-236, 2016
ISSN 2079-2077

DOI: 10.5829/idosi.ejas.2016.8.4.22971

Tampering Detection and Hash Coding Self-Recovery in Digital Image Protection

M. Aruna and Dr. N. Srinivasan Narayanasamy

Department-MCA, Faculty of Computing, Sathyabama University, Chennai-600119, Tamilnadu, India

Abstract: Image forensics field has widely been applying Watermarking algorithms during the recent period. Protecting images from tampering is one among such varied forensic applications. To achieve this purpose, some watermarking algorithm needs to be designed with regard to tampering of image: 1) identifying tampered area present in the image that has been received and 2) restoring the information that has been lost in tampered regions. The purpose of this study is to identify the tampered zones present in the image that has been received and to restore missing information in tampered areas. The hacker adds unidentified alterations in the area of authentic images during tampering stage. Hence, an image gets damaged with regard to its identity. Check bits are normally used to detect this while reference bits may be used for carrying information regarding the image on the whole. It is possible to model and deal image tampering as an error of deletion. During the stage of watermark embedding, the authentic image gets channel coded, while the resultant bit stream gets protected with suitable channel encoder. In the process of image recovery, deletion locations identified usage of check bits assist channel deletion decoder for restoring the authentic channel coded image. The scheme suggested by us outshines other recent techniques considerably with respect to image quality as far as watermarked and restored image are concerned. Whereas quality of watermarked image is attained using reduced bit-budget regarding watermark quality of image recovery can be improved substantially and subsequent to constantly performing devised channel and channel codes

Key words: Image watermarking · Image tampering protection · Self-recovery · Haar Wavelet

INTRODUCTION

Image authentication has become an attracting topic of research in the recent past as it is possible to modify or tamper multimedia data present in the digital form easily with the assistance of various tools for image processing, regardless of it being malicious or otherwise. By adopting digital delicate watermarking that is a method of embedding digital signature on an image [1], the originality and integrity of such digital images may well be assured. Many self-restoration watermarking strategies have been suggested for rebuilding tampered regions. These strategies impart image block factors to take the place of watermark payload connected to other block or blocks of image. Lin *et al*. [2] suggested that the soundness of a block of image was established using more authentication data available inside a block. In particular, both recovery data and authentication data are included in the charge of watermark. While a block implants authorization data in it, recovery data gets embedded in some other block. In the case of huge quantity of some image having been tampered, the general quality of recovered image may be poor. For improving the restoration quality, a dual watermarking approach was suggested by Lee and Lin [3]. Two different watermark copies showing the complete image are maintained in this strategy and they offer a second possibility of block restoration in the event of one copy getting destroyed. The performance evaluation of one type of self-restoration delicate watermarking strategy that employs an enhanced neighborhood definition method for detecting the tampering was presented by He *et al.* [4]. A digital image watermarking approach provides answers to image authentication, copyright and other such issues. Watermarking consists of disintegrating the actual image known as the cover image by using certain wavelet transforms [5] as well as implanting watermark on to any of the available sub bands (LH,LL,HH,HL). The image

Corresponding Author: M. Aruna, Department-MCA, Faculty of Computing, Sathyabama University, Chennai-600119, Tamilnadu, India.

thus acquired is known as watermarked image (i.e.,Stego Image). This particular image gets transmitted through a channel wherein different noises impact the watermarked image [6]. Implanted watermark is extracted out of the watermarked image at the side of the receiver. Discrete Wavelet Transform (DWT) is used for watermark implanting. DWT, the wavelet transform uses Dydic Filters for decomposing M N image into N-Levels. It is possible to implant watermark on to any of the sub bands. Inverse Discrete Wavelet Transform (IDWT) [7] is being used for watermark extraction. Predominantly used frequency-realm transforms are the Discrete Cosine Transform (DCT), the Discrete Wavelet Transform (DWT) and the Discrete Fourier Transform (DFT). DWT however finds more frequent usage in the process of watermarking with digital image because of its exceptional spatial localization as well as multi-resolution qualities that are similar in nature to theoretical models present in the human ocular system [8]. From the time it emerged, Digital image watermarking is found to have been applied widely for authentication of image and protection of copyright. Anyhow, it finds its application being extended in connection with digital image self-restoration, wherein the tampering-caused loss of original images content is retrievable by using information implanted inside the particular image itself. The normal method in approaches like these is to implant an illustration of the authentic image into the very image itself [9]. By making use of appropriate channel codes, this information may be guarded from tampering. It has recently been proved; anyhow, that digital image self-restoration may be prototyped as some channel coding issue [10]. And in this method, the information regarding channel encoded image may be channel coded by making use of appropriate codes and implanted on to it. Hence, the Tolerable Tampering Rate (TTR) and the retrieved image quality are dependent on the bit-rate devoted to the channel and origin code bits, correspondingly. Since watermarking with digital image that is founded on the transform realm can be implanted watermark with regard to carrier image dimensional energy scattering of each pixel, the watermark may have possibility to attain powerful anti attack capability. Due to this, algorithm of image watermarking related to transform realm is found to contain high value for research and practicability. Presently, major portion of research about the algorithm of watermarking with digital image process is found to have been founded on the transform realm, transform realm classical DCT realm, DWT realm and the DFT realm. Koch has taken a head start in one algorithm of - watermarking with digital image that is founded on DCT realm. In this, watermarking information gets implanted into selected medium frequency DCT coefficients. As JPEG image compaction is employed for achieving the DCT, this algorithm is found to have robustness from JPEG compression.

Related Works: This section deals with the review about digital watermarking that is employed for images. This explains about the earlier that has been done about digital watermarking under DWT method and other methods, including the study of different watermarking strategies and their outcomes. Mistry [11] initiated digital watermarking strategies spatial realm (such as LSB) and transform realm (such as DWT, DCT) approaches. Spatial realm happens to be the common image space wherein a positional change in image projects directly to a positional change in space. Example of this is Lowest Significant bit (LSB) approach. Transform realm method first transforms the authenticated image into frequency realm using Discontinuous Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), or Fourier transform and hence produces watermarked image of high quality. Researchers have realized that transform watermarking proves relatively far better than spatial realm encoding. Two LSB techniques were proposed by Van *et al.* [12]. While the first one makes a replacement of the images LSB with any pseudo-noise (PN) order, the second one will add a PN order with the LSB of the particular data. Patchwork, another such LSB-concealing approach, selects n pairs (ai, bi) corresponding to the points found in a particular image and keeps increasing ais brightness with one unit whereas decreasing bis brightness simultaneously. The fact that the data being highly vulnerable toward noise and it may be easily destroyed hinders this study. Moreover, quality of image may get degraded due to the watermark. A watermarking strategy founded on DCT was suggested by Blossom *et al*. [13]; it offers enhanced obstruction to image handling attacks like noise, rotation, JPEG compression, translation and so on. In this particular scheme, watermark is implanted in the medium-frequency band related to DCT blocks that carry low frequency elements while elements of high frequency range sub band stand unused. By adjusting coefficients of DCT and by making use of private key, watermark can be inserted. Extracting the watermark can be done making use of that private key itself, avoiding turning to the authentic image. It has been shown by performance analysis that watermark happens to be robust. A powerful digital watermarking strategy was proposed by

W.Hong *et al*. [14] for protection of copyright of digital images with regard to sub-sampling. Watermark is treated as binary image that is implanted in coefficient of discrete transform pertaining to host image; it is not being used with actual image. They have adopted chaotic map with watermarked image in this strategy. Anyhow, the resultant of the watermark image happens to be robust against attack and good. Xia *et al*. [15] suggested one kind of watermarking strategy that is founded on Discrete Wavelet Transform (DWT). This watermark, prototyped as a Gaussian noise, got added with the high and medium frequency packs of the image. In this, the process of decoding included picking up the DWT of any possibly marked image. Portions of watermark were derived and coordinated with portions of the actual watermark. Watermark was identified in case the cross-comparison was found to be above some threshold. If not, the image got broken-up into thinner and thinner bands till such a time that the entire derived watermark was coordinated with the complete actual watermark. It has been shown by performance evaluation that the DWT is far more powerful to attack, when compared to DCT. The trouble with the suggested technique is that it is vulnerable to several geometric assaults. Akhil *et al.* [16] suggested a powerful image watermarking method founded on the 1-level DWT (Discrete Wavelet Transform). The technique implants invisible watermark with the prominent aspect of the actual image by making use of the technique of alpha blending. From the output of experiment, it is understood that implanting and deriving of watermark relies on the alpha value only. All outputs attained for the watermark and the restored images are found to be synonymous with the actual images. G.Bhatnagar *et al.* [17] proposed one half-blind reference watermarking technique founded on discrete wavelet transform (DWT) and singular value decomposition (SVD) for protection of copyright and authenticity. The watermark used by them was a logo image of gray scale. For watermark implanting, their algorithm converted the actual image subsequently into wavelet realm and one reference substitute-image is created by making use of wavelet coefficients and directive contrasts. After that, their algorithm implanted the watermark with benchmark image by altering the unique values of benchmark image with the use of unique values pertaining to the watermark. M. Barni *et al.* [18], then, have presented an improved version of watermarking that is wavelet-based, under pixel-wise masking procedure. It is founded on masking watermark in accordance with the HVS characteristics. The watermark gets added adaptively with the bands with largest details. Watermark weighing exercise is then calculated as one plain product of the data derived from the HVS model. Then the watermark is identified by comparison. The presented technique is robust against many assaults but then this method is complicated compared to other techniques of transform. Kundur *et al.* [19] disintegrated binary logo via DWT. Here, the watermark gets scaled with a salience element, gauged on a piece by piece basis, based on noise sensitivity of local image. After that, it gets added to alternate packs of DWT disintegration of actual image. Hence, visual masking is accomplished only up to block resolution. By appropriately quantizing the detail bands coefficients, binary code gets implanted. The implanted binary code may be assessed using analysis of coefficients quantization, to restore watermark. Having assessed the code, it can be coordinated and the result gets compared to some threshold selected based on some false positive possibility. Many of the techniques found in this study are highly complicated and they include multi-faceted performance phases. In this research, we have attempted to introduce a new easy method for hiding one grayscale image inside another such grayscale image by making use of 3-level DWT along with alpha-blending strategy for security process.

Proposed Work

Overall Architecture: In the study, we are identifying an images tampered area and restoring the information that has been lost in a given image. Giving the actual image as input, we encrypt the actual image by using DWT. When encryption is over, the actual image decrypts the image by making use of IDWT. The decrypted image may then will compress with the use of Haar Wavelet channel coding method. Permuting the image is then done; during permutation, the actual m x n level image pixel changes to the structure of n x m. Information about the complete image is carried by the reference bits. Conceal the image with the use of hash value and create secret key in channel coding. Permute the image in connection with security again, after the channel coding. In the tampering stage, it may be possible for hacking the image. Then the detected changes will get executed in the actual image during this stage. Tampered zone of the image will then be detected with the use of check bits. For reconstructing the image, apply the process of inverse permutation now. Quality of the image might be improved by the watermarked image.

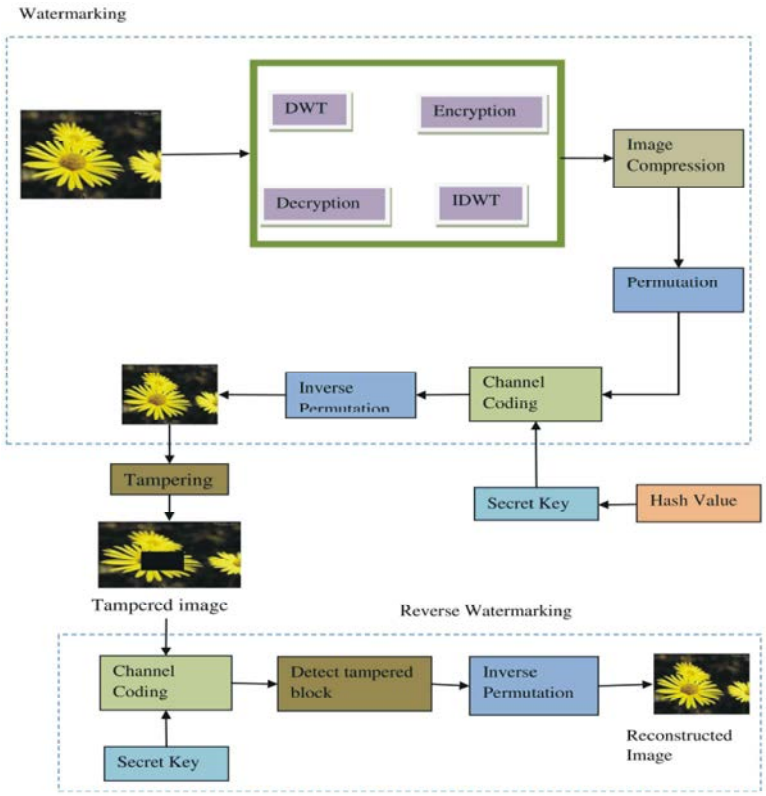

Fig. 1: Image Protection and Self-recovery

Channel Coding: Haar Wavelet is exercised for channel encoding strategy. Haar Wavelet is one implanted compression approach that allows truncation of resulting bit stream in the desired rate. The image gets uploaded in the Haar Wavelet Compression Primary step. Haar Wavelet algorithm is being used for designing an image in 8-bit format. It is one of the wavelet transform types. Haar Wavelet and wavelet transform channel coding approach are used for compressing the actual image efficiently. Hence, three parts are included in the watermark in the algorithm that we employ: check bits, channel encoding bits and the channel code uniformity bits. Channel encoding bits that take the role of reference bits may be considered as bit stream in Haar Wavelet -compressed actual image at any rate desired. For surviving tampering deletion, reference bits may be channel coded for producing carrier code bits. At receiver side, check bits may be used for determining the deletion location for channel deletion decoder. For finding the compressed form of the actual image, the result of the channel decoder has to be channel decoded. From this procedure, it can be seen that our chosen algorithm outshines other existing approaches with relation to similar watermark payload with 3 bits in a pixel (bpp), by selecting suitable parameters for channel and channel decoding.

Discrete and Inverse Discrete Wavelet Transform: Discrete Wavelet Transform (DWT) means wavelet transforms in which wavelets get discretely sampled. This transform is founded on wavelet matrix that can be calculated far quickly when compared to Fourier matrix that is analogous. Wavelet compression can be defined as one type of data compaction that is appropriate with relation to image compression (at times, audio compression as well as video compression). For changing the locations of pixel as well as the values in actual image, DWT encryption may be used. It implants the processed actual image into one wavelet sub-band with respect to another shield image and executes inverse wavelet transform for attaining the image that has been encrypted. Correct extraction of the processed actual image from the particular encrypted image is ensured by the wavelets. It is assured by later ones that the actual image may then be reconstructed correctly.

Permutation: The method of permutation is found to work as under: The given plain image gets disintegrated into blocks, with each one containing a particular number of given pixels (blocks of 4 pixels 4 pixels). Permutations prior to and post channel coding can be created by using two keys, namely, k1 and k2, these two being extracted from one secret key, namely, K, that will be known to implanting stage 9transmitter end) as well as image rebuilding stage (receiver end), for guaranteeing our algorithms security. In fact, the bc bits actually belong to certain other blocks in which indices and rows are changed into binary stream pertaining to brc bits known as position bits. The said brc position bits, in combination with a bm = nm B2 MSB of bits belonging to each block will then be used in place of input on a hash creator algorithm (MD5 in this case), for producing bh = nhB2 hash bits. An indiscriminate binary key with length bh that is fixed upon the complete image is created at the implanting stage. The key can be XORed using hash bits for generating bh amount of check bits. Such particular bh check bits, combined with the bc carrier code bits from each block can be spread upon the block that will result in the replacement of last nw = nc + nh amount of lowest significant bits having each pixel pertaining to the actual image.

Tampering: The hacker adds undetected alterations in the area of actual images in the Tampering stage. This way, the images identified will get damaged.

Detection and Recovery: The watermark's bit stream itself is broken into a level of bh = nh B2 to check bits and then bc = nc B2 of channel code bits. Bits with brc position combined by bm MSB bits can be used to create bh level of hash bits. For each of the blocks, XOR of the computed hash bits as well as derived check bits get recorded. In the case of unmodified blocks, such bit stream will equal the indiscriminate key that is used in implanting stage. So, one can locate tampered blocks through comparison of the results and by spotting out the odd ones. Carrier code bits go through appropriate inverse permutation after the particular tampered blocks have been located. The condensed image bit flow is accessible at the decoders output which can transmitted the past origin decoder after going through suitable inverse permutation. Then, the rebuilt image may be made using the replacement of the tampered blocks with their matching blocks located in the channel decoders output. Evidently, the ingredients belonging to the image received inside preserved blocks do not get replaced with matching information derived from the recovered image.

Algorithm 1: DWT:

- Compute dimensionality of an image.
- Generate secret key from permutation and apply wavelet transformation (split Z, Dc and Ds components for color images) based on the generated secret key.
- Group wavelet coefficients into m x m blocks Ck from the encrypted image of N x M pixels.
- Compress Ck by using loss JPEG coding based on DWT.
- The n coefficients of the consequent blocks Ck+1,... , Cl can be used to insert the current bits of the compressed block Ck.

Algorithm 2: IDWT:

- Based on DWT, JPEG decoding can be presented to decompress the blocks.
- Extract the inserted block of Ck+1,..., Cl coefficients |Di(i, j)|. T.fom the consequent blocks such that Embedded-bit = 1 Di(i, j) = odd, 0 Di(i, j) = even
- Apply JPEG decoding based on DWT for inserted block.
- Repeat 1-3 until l > N x M / m x m, l = l + 1.
- Create DWT image form from extracted and original blocks.
- Apply IDWT.
- Apply inverse of wavelet transform on decompressed image.

RESULT AND DISCUSSION

The Figure 2 shows the DWT of an image. The original image will be uploaded to encrypt. Then the image will be encrypted using DWT[20].

The Figure 3 shows the Permutation of an image. It is an arrangement of image parts the original image will be change.

The figure 4 shows the hacked image. In hacking stage, the hackers make change in an original image.

The figure 5 shows retrieval of an original image. Using secret key the original image can retrieve from hacked image.

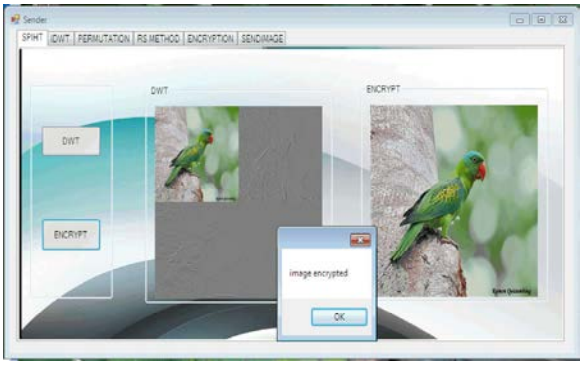

Fig. 2: DWT of an Image

Fig. 3: Permutation

Fig. 4: Hacked Image

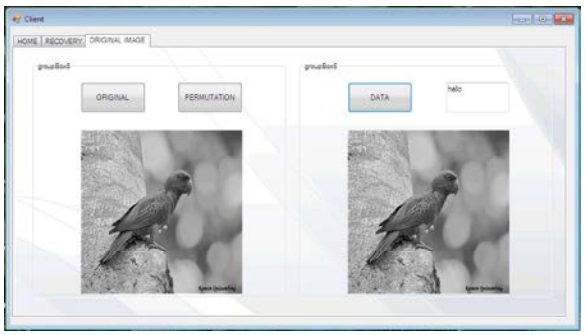

Fig. 5: Retrieval Original Image

CONCLUSION

This study introduces an innovative method that is founded on unequal fault protection for generating images that are tamper-proof. Actual image is condensed with Haar Wavelet encoder; the resultant bit stream then gets channel coded for exhibiting robustness from tampering. Under this method and as per one dynamic programming moderation strategy, channel code uniformity bits can be moderately allotted to Haar Wavelet bit-planes so that bits with more priority get better protection. Resulting from this, the restored images quality is high with low tampering rate and it will be possible to recover tampered image in spite of tampering rates being high. It is confirmed from simulation results that the suggested approach is superior to other recent methods when it comes to the restored images quality and also tampering rate.

REFERENCES

1. Fridrich, J., 2002. Security of Fragile Authentication Water-Marks with Localization, of SPIE 4675, Security and Watermarking of Multimedia Contents IV, 691: 691-700.
2. Lin, P.L., C.K. Hsieh and P.W. Huang, 2005. A Hierarchical Digital Watermarking Method for Image Tamper Detec-tion and Recovery, Pattern Recognition, 38(12): 2519-2529.
3. Lee, T.Y., S.F. Lin and D. Dual, 2008. "Watermark for Image Tamper Detection and Recovery," Pattern Recognition, 41(11): 3497-3506. doi:10.1016/j.patcog.2008.05.003.
4. He, H.J., F. Chen, H.M. Tai, T. Kalker and Jiashu Zhang, 2012. Performance Analysis of A Block-Neighborhood-Based Self-Recovery Fragile Watermarking Scheme, IEEE Transactions on Information Forensics and Security, 7(1): 185-196.
5. Nagaraj V. Dharwadkar and B.B. Amberker, 1989. International Journal of Image Processing Determining the Efficient Subband Coefficients of Biorthogonal Wavelet for Gray level Image Watermarking International Journal of Image Processing, 4: 2.
6. Chu, W., 2003. DCT-Based Image Watermarking Using Subsampling, IEEE Trans. Multimedia, 5(1): 34-38.
7. Lin, S. and C. Chin, 2000. A Robust DCT-based Watermarking for Copyright Protection, IEEE Trans. Consumer Electronics, 46(3): 415-421.

8. Guangnan Kevitt Zhang and Wang Shushun, A Blind Watermarking Algorithm Based on DWT for Color Image.
9. Deng, F. and B. Wang, 2003. A novel technique for robust image watermarking in the DCT domain, in Proc. of the IEEE 2003 Int. Conf. on Neural Networks and Signal Processing, 2: 1525-1528
10. Zhang, X., Z. Qian, Y. Ren and G. Feng, 2011. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction, Information Forensics and Security, IEEE Transactions on, 6(4): 1223-1232.
11. Sarreshtedari, S. and M.A. Akhaee, 2014. Source-channel coding approach to generate tamper-proof images, in Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on, pp: 7435-7439.
12. Darshana Mistry, 2010. Comparison of Digital Watermarking methods, 21st Computer Science Seminar SA1-T1-7, IJCSE.
13. van Schynde, R.G., A.Z. Tirkel and C.F. Osborne, 1994. A digital watermark, in Proc. IEEE Int. Conf. Image Processing (ICIP).
14. Blossom Kaur, Amandeep Kaur and Jasdeep Singh, 2011. Steganographic Approach for hiding Image in DCT Domain, International Journal of Advances in Engineering and Technology.
15. Hong, W. and M. Hang, 2006. Robust Digital Watermarking Scheme for Copy Right Protection, IEEE Trans. Signal Process, l2: 1-8.
16. Xia, X., C. Boncelet and G. Arce, 1997. A Multiresolution Watermark for Digital Images, Proc. IEEE Int. Conf. on Image Processing.
17. Shing Akhil Pratap and Agya Mishra, 2011. Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering.
18. Bhatnagar, G. and B. Raman, 2008. A new robust reference watermarking scheme based on DWTSVD, Elsevier B.V. All rights reserved.
19. Barni, M. and F. Bartolini, 2001. An Improved Wavelet Based Watermarking through Pixel wise Masking, IEEE transactions on image processing.
20. Kundur, D. and D. Hatzinakos, 1998. Digital Watermarking using Multiresolution Wavelet Decomposition, Proceedings, IEEE International Conference Acoustic, Speech, Signal Processing.