www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.17827-17832

A Novel Digital Watermarking Approach for Accurate Authenticati on Using of Integer Wavelet Transform Coefficients

P.Sayanna[1], B. Laxmi priya [2]
[1] Associative Professor, ECE Department, SRCW, Nizamabad, India
[2]M.Tech Student, MATLAB, SRCW, Nizamabad, India
sayanna6367@gmail.com[1], laxmipriya428@gmail.com[2]

Abstract: The prominence of digital image processing domain has been increased from last few decades due to its advanced res earch areas such as medicine, biometrics, military, robotics etc. In this work an important issue has taken as area of research i .e. protecting the privacy information from the unauthenticated users either as accidental or incidental ways. Although tremen dous progress has been made in the past years but still protecting the privacy information is concerned area in the field of secu rity. A novel image authentication scheme for gray scale images are implemented in this work and the process of the embeddin g digital watermark is carried by performing the quantization process on the image. The novel things implemented in the propo sed work is detection of tampered parts of the image and to detect minute modification of an image and to embed the watermar k mid frequency band of a second level DWT transform was used. An approximation of the original image based on LL band w as stored as a recovery mark for restoration of the image. Watermarked image has achieved a good PSNR value of 40 dB comp ared to original cover image. Restored image quality was also very good with a PSNR of more than 35 dB compared to unmodi fied watermarked image even when 25% of the received image is cropped. Finally the simulation results reveals that the propos ed method provides the reliable balance between fidelity of the watermarked image and the quality of the restored image.
Keywords: Authentication, Tampered part detection, Privacy protection, Image restoration, IWT

1. INTRODUCTION

Tampering of digital media and its detection has been an int eresting problem since long time. Its importance has increas ed with the stepping up of the use of digital media on the Int ernet. The volume of data transmission especially that of im ages and videos, has gone up exponentially and has naturall y drawn the interest of many including, unfortunately, fraud ulent persons who would tamper with the transmitted data to suit their purpose. The detection of tampering followed by r estoration of the original image is hence an important task. Most of the research carried out so far has been of tamper de tection, while more recent work includes recovery of the im age as well.

A number of digital watermarking schemes have been report ed during the past decade for different purposes and conside rations. An image tamper detection and recovery system has been developed based on the discrete wavelet transform (D WT) technique where some information has been extracted as the Eigen value of the image and is embedded in the midd le-frequency band of the frequency domain. Such embeddin g has been used for tamper detection and localization.

A novel fragile watermarking scheme based on chaotic syste m for image authentication or tamper proofing is proposed. The watermark is generated by using pixel values as input v alues of a chaotic system, and a secret key controls a set of p arameters of the chaotic system. A quantization function is i ntroduced to embed and detect watermarks. This method can effectively detect minor alteration in a watermarked image.

(A) Overview of digital watermarking

Watermarking is a sub-discipline of information hiding. It is the process of embedding information into a digital signal i n a way that is difficult to remove. It's providing copyright p rotection for intellectual method that's in digital format. Dig ital watermarking is an important branch of the information hiding technology. In recent years as digital information is c

irculating through the world by means of the rapid and exten sive growth in internet technology, therefore there is a need t o develop newer techniques to protect copyright, ownership and content integrity of digital media. Digital Watermarking technology allow users to embed digital information into au dio, images, video and printed materials in a way that is pers istent, imperceptible and easily detected by computers and d igital devices, shown in figure 1.1.

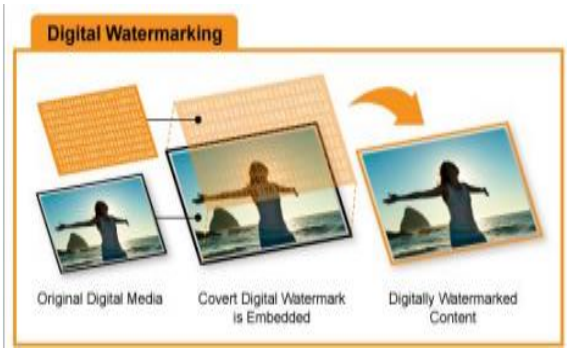

Figure 1: Digital watermarking

Digital watermarking is a promising solution for co pyright protection, it promises extra robustness n embedded information. The embedded information is called watermark s. The embedded information is called watermarks. We have used a digital watermark which is transparent, invisible info rmation pattern that is inserted into a suitable component of the data source (image) by using a specific computer algorit hm.

(B) Properties of digital watermarking

- **Imperceptibility:** The difference between the origi nal image and the watermarked image should be un known to the human observer.
- **Trustworthiness:** A watermarking scheme should guarantee that it is impossible to generate counterfe it watermarks and should provide trustworthy evide nce to protect the rightful ownership.
- **Robustness:** Watermarks should be robust to com mon signal processing and intentional attacks. The watermarks should still be extracted from the attack ed watermarked image.
- **Security:** unauthorized parties should not be able t o read or alter the watermarking**.**

Using wavelet transform in the digital image processing has gained popularity in recent times. One of the most popular a pplications of discrete wavelet transform is in the JPEG2000 image compression scheme whereas its predecessor JPEG s tandard was DCT based. Discrete wavelet transform is also being used in the domain of digital watermarking. Kundur a nd Hatzinakos proposed a fragile watermarking scheme for t amper proofing, where the watermark is embedded by quant izing the DWT coefficients. One of the main advantages of using DWT is its power in multi-resolution analysis. This ca pacity was exploited in the proposed scheme to encode a lo w resolution version of the image and embed it in the origin al image. Spread spectrum watermarking method has been a popular choice for watermarking digital media with the purp ose of protecting owner's copyright. However, it was found empirically that for authentication purpose quantization base d watermarking performs better than spread spectrum water marking.

This paper proposes a novel method for authentication of gr ayscale image by using digital watermarking. The proposed method embeds a digital watermark in a grayscale image by the process of quantization of the grayscale values of the pix els of an image. To embed the watermark, mid frequency ba nds of a second level DWT transform was used to ensure bot h the fidelity of watermarked image and the accuracy of tam per detection. A low resolution version of the original image was stored in the LSB of the watermarked image to recover a tampered image. The method designed with a goal to ensur e a better balance between the fidelity of watermarked imag e and the quality of reconstructed image.

2. LITERATURE SURVEY

Veysel Aslantas 2008 presented an optimal watermarking s cheme based on singular-value decomposition (SVD) using genetic algorithm (GA). The singular values (SVs) of the ho st image are modified by multiple scaling factors to embed t he watermark image. Modifications are optimized using GA to obtain the highest possible robustness without losing the t ransparency. Experimental results showed both the significa nt improvement in transparency and the robustness under att acks. Based on existing experiences to evaluate the applicabi lity of robust watermarking, it is generally agreed that three parameters or requirements, including the quality of waterm

arked contents, the survivability of extracted watermark afte r deliberate or unintentional attacks, and the number of bits e mbedded, need to be considered. However, performances rel ating to these three parameters conflict with each other, and the trade off must be searched for.

Hsiang-Cheh Huang 2009 has taken all the three requireme nts into consideration, and add the flexibility to meet the spe cific design in implementation. With the aid of genetic algor ithm, they designed an applicable system that would obtain t he good quality, acceptable survivability, and reasonable cap acity after watermarking. Simulation results presented the ef fectiveness in practical implementation and possible applicat ion of the proposed algorithm.

Zorana Bankovic 2009 demonstrated the effectiveness of u sing GA's in fast searching of the space of the possible solut ions . A high detection rate was achieved after a relatively s hort period of training time. Also the by retraining, the syste m becomes highly adaptable. As the GA's are inherently par allel in operation there is a possibility of using reconfigurabl e hardware with the implementation cost much lower. At the same time GA's can search the solution space in multiple di rections at once.

Sanjeev Kumar 2009 presented a digital watermarking alg orithm in discrete wavelet transform (DWT) domain for ster eo image coding. First, a disparity-image was computed fro m the pair of stereo images using a frequency domain based matching criteria. Later, this disparity-image was used as a watermark and embedded into the degraded host (left stereo) image based on a modifying singular values concept. The h ost image was degraded using Arnold transform. Finally, rea l coded genetic algorithm (RCGA) was used to estimate the optimal order of Arnold transform and the strength of water mark to fulfill the tasks of security, invisibility and robustne ss in proposed algorithm. In proposed algorithm, a legal user can retrieve the embedded watermark (disparity-image) and so able to recover 3-D information and right image of the st ereo- pair. Experimental results were presented to evaluate t he performance of proposed algorithm in terms of accuracy and robustness.

Chih-Chin Lai 2009 presented a robust digital image water marking scheme based on singular value decomposition (SV D) and micro-genetic algorithm (micro-GA). In an SVD-bas ed watermarking scheme, the singular values of the cover im age are modified by considering multiple scaling factors to e mbed the watermark image. Determining the proper values o f scaling factors is not an easy task. They viewed it as an opt imization problem and apply the micro-GA to efficiently obt ain the values. Experimental results showed that the propose d approach has good performance against several attacks.

Chen Yongqiang 2009 presented a DWT domain image wa termarking scheme to meet the watermarking properties: sec urity, imperceptibility and robustness. In the scheme, water mark comes from a meaningful binary image encrypted by t wo-dimensional chaotic stream encryption that has more sec urity. In the procedure of watermark embedding, the waterm ark is embedded into host image through selecting and modi fying the wavelet coefficients using Genetic algorithm with a simple fitness function to improve the imperceptibility of watermarked image. In order to identify the owner of extract ed watermark, Synergetic Neural Network is used in the wat ermarking identification to overcome the limitation of correl ation analysis or the human sense organ after some attacks. The results of their scheme realization and robust experimen ts showed that the scheme has preferable performance.

Jiann-Shu Lee 2009 proposed a watermarking algorithm fo r uncompressed video based on Quantization Index Modulat ion (QIM) and differential energy. The Differential Energy Watermarking (DEW) algorithm has been demonstrated as a n effective video watermarking algorithm;while in some sce narios, DEW algorithm cannot provide enough robustness a nd fidelity. This problem has been solved by above authors. The experimental results indicated that the proposed algorith m is more robust than original DEW and modified low-frequ ency DEW for lossy compression and transcoding, while ma intaining high fidelity.

3. PROPOSED METHOD

(A) Integer Wavelet Transform

Discrete Wavelet Transform (DWT) is suitable for identifyi ng the areas of the cover image where a watermark can be i mperceptibly embedded because of its excellent SPATIO fre quency localization properties. The integer wavelet transfor m is a specialized version of general DWT which maps inte gers to integers. The advantage of using integer wavelet tran

sform is that it can be implemented with only fundamental a rithmetic operations. In integer wavelet transform, the image is first decomposed in 4 sub bands, LL1, HL1, LH1 and HH 1respectively.

The LL1 band is further decomposed into four sub bands obtaining LL2, HL2, LH2 and HH2. This level wise d ecomposition can be performed as many times as required. The LL band, or more specifically LL k band of DWT conta ins the low frequency components of the image and it can be treated as an approximation of the image. Here k indicates t he maximum level of decomposition done on the image. Mo st of the energy of the image is concentrated in this band. An y modification done to this band is visually most perceptible . The HL and LH band of DWT contains horizontal and vert ical components of the image and the HH band is called the diagonal band. These latter three bands are high frequency b ands. These bands contain the detail information of an imag e like the edge information. The following figure depicts a t wo level decomposition of an image using integer wavelet tr ansform.

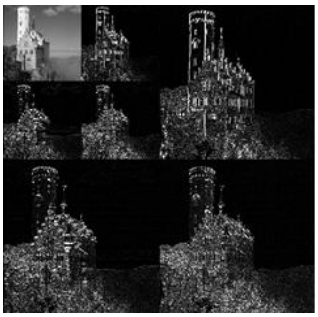

Figure 2: Different bands in wavelet transform

(B) Proposed Method Analysis

In the proposed method, the HL2and LH2bands were used t o embed a watermark to the image. Any or both of the bands could be used for embedding the watermark. However, in th e proposed method both of the bands were used to reduce th e false positive signal. LL band was not used for embedding the watermark to ensure high fidelity of the image. HH band is generally avoided as it contains important edge informati on of the image. The LL1component was also used in the pr oposed scheme as an approximation of the original image an d it is encoded into the LSBs of watermarked image as a rec overy mark. This recovery mark is extracted from the trans mitted image. If any tampering is detected in the transmitted image then this extracted recovery mark is used to restore th e image to its original state. To obtain wavelet transform ban d we used Haar wavelet with lifting scheme. Furthermore, th e operation is done in only integer domain to ensure lossless decomposition. It also ensured high computational speed of t he proposed scheme.

In the proposed method DWT coefficients of HL2and LH2 b ands were quantized. The technique used for quantizing the DWT coefficients is as follows: Let **d** is the amount of modu lation in DWT coefficient after quantization and **b** is the val ue of the watermark bit in the reference pattern that will be e mbedded. Also, let **p** is the DWT coefficient to be modulate d and **m** is the modulated DWT coefficient. Now, **m** will be modulated using following algorithm:

```
f = floor(p/(2*d))
c = ceil(p/(2*d))
if |v-f| <= |v-c|
        if b == 0
                m = f*2*d
        else
                m = f*2*d + d
        endif
else
        if b == 0
                m = (f+1)*2*d
        else
                m = (f+1)*2*d + d
endif
endif
```

A binary image was taken as the watermark. The resolution of this image should be one fourth of the cover image in eac h dimension. This watermark image is embedded into the co ver image using the following algorithm

1. Divide the image into 8×8 sub blocks

2. Compute 2-level DWT for each of the block

3. LL1band of a block X is embedded into the LSB of a diff erent block Y as a recovery mark. The location of block Y is

determined by using a secret watermark key which should b e available to the watermark detector.

4. Modify the DWT coefficients of the HL2and LH2 band a ccording to the algorithm described above. Each bit of the w atermark image is embedded in one coefficient of HL2band and in one coefficient of LH2 band

5. Compute Inverse DWT for each block to get the watermar ked image

Let **x** is a DWT coefficient of received image. Then, waterm ark bit **b** from this coefficient was extracted using the follow ing algorithm:

```
if |x mod 2*d| <= t
        b = 0;
else
        b = 1;
end
```

Here**,, t** is a predefined threshold value. The watermark extr action and recovery process is as follows:

1. Divide the image into 8×8 blocks
2. Extract Recovery mark from each block of the image
3. Compute 2-level DWT for each of the block
4. Extract Watermark from HL2and LH2band of each of the block of the image
5. Compute correlation coefficient of extracted watermark a nd original watermark for each block
6. If the correlation between extracted watermark and origin al watermark is larger than the threshold then mark the bloc k as authentic, otherwise mark the block as inauthentic or ta mpered.
7. Replace the tampered blocks using recovery mark

4. SIMULATION RESULTS

Figure 3: Cover image

Figure 4: Watermarked image

Figure 5: Watermarked image

Figure 6: Recovery image

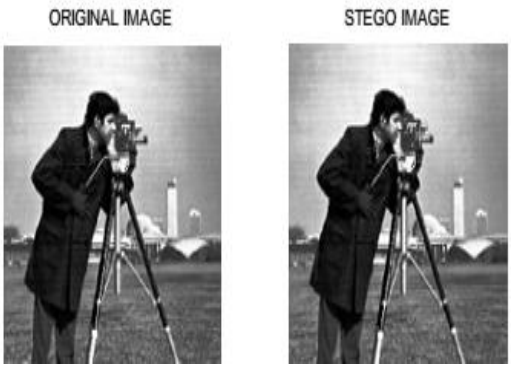

Figure 7: Method 1 STEGO IMAGE

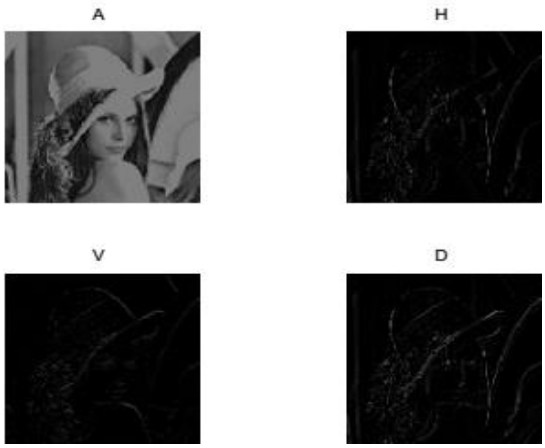

Figure 8: Method 2 DWT decomposition

5. CONCLUSION

The proposed method is computationally fast as it uses only integer based operation. Watermarked image in the propose d method showed good PSNR for the standard image which indicates a very acceptable fidelity. Tampered location of an inauthentic image was successfully identified by the propos ed algorithm and the quality of the recovered image was als o quite satisfactory. Proposed method ensured a better balan ce between the fidelity of watermarked image and the qualit y of the recovered image as compared to the method propos ed

6. REFERENCES

[[1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalk er, Digital Watermarking and Steganography, Second Editio n, p. 375, 2008

[2] C.-Y. Lin and S.-F. Chang, “A robust image authenticati on method distinguishing JPEG compression from malicious manipulation,” IEEE Trans. Circuits Syst. Video Technol., vol. 11, no. 2, pp. 153–168, Feb. 2001.

[3] P. W. Wong, "A watermark for image integrity and own ership verification," in Proceedings of IS&T PIC Conferenc e, (Portland, OR), May 1998.

[4] P. W. Wong, "A public key watermark for image verific ation and authentication", in Proceedings of ICIP, (Chicago, IL), October 1998.

[5] P. W. Wong and N. Memon, “Secret and Public Key Ima ge Watermarking Schemes for Image Authentication and O wnership Verification”, IEEE Transactions on Image Proces sing, vol. 10, no. 10, pp. 1593–601, 2001.

[6] J. Fridrich and M. Goljan, "Protection of Digital images Using SelfEmbedding", Symposium on Content Security an d Data Hiding in Digital Media, New Jersey Institute of Tec hnology, May 14, 1999.

[7] J. Fridrich and M. Goljan. “Images with Selfcorrecting C apabilities,” in Proceedings of the IEEE International Confer ence on Image Processing, volume 3, pp. 792–796, 1999.

[8] K. Ke, T. Zhao & O. Li, "A Restorative Image Authentic ation Scheme with Discrimination of Tampers on Image or Watermark", 4th International Conference on Multimedia an d Ubiquitous Engi-neering (MUE), pp. 1-5, 2010.


B.Laxmi priya, who has specialization in M.Tech and currently an M.Tech Student of Department of ECE,SRCW.


P.sayanna, specialization in M.Tech and working as an Associate Professor at SRCW, Hyderabad and his areas of interest are Embedded Systems.