A NOVEL DIGITAL WATERMARKING APPROACH FOR ACCURATE AUTHENTICATION USING OF INTEGER WAVELET TRANSFORM COEFFICIENTS

Boddula Madhavi 1, Dr. Rajkumar L Biradar2, Dr. K. Rama Linga Reddy3
Department of ETM, 1 Associate professor2, H.O.D. (ETM)3
G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, INDIA

Abstract: The prominence of digital image processing domain has been increased from last few decades due to its advanced research 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 tremendous progress has been made in the past years but still protecting the privacy information is concerned area in the field of security. A novel image authentication scheme for gray scale images are implemented in this work and the process of the embedding digital watermark is carried by performing the quantization process on the image. The novel things implemented in the proposed work is detection of tampered parts of the image and to detect minute modification of an image and to embed the watermark mid frequency band of a second level DWT transform was used. An approximation of the original image based on LL band was stored as a recovery mark for restoration of the image. Watermarked image has achieved a good PSNR value of 40 dB compared to original cover image. Restored image quality was also very good with a PSNR of more than 35 dB compared to unmodified watermarked image even when 25% of the received image is cropped. Finally the simulation results reveals that the proposed 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 interesting problem since long time. Its importance has increased with the stepping up of the use of digital media on the Internet. The volume of data transmission especially that of images and videos, has gone up exponentially and has naturally drawn the interest of many including, unfortunately, fraudulent persons who would tamper with the transmitted data to suit their purpose. The detection of tampering followed by restoration of the original image is hence an important task. Most of the research carried out so far has been of tamper detection, while more recent work includes recovery of the image as well.

A number of digital watermarking schemes have been reported during the past decade for different purposes and considerations. An image tamper detection and recovery system has been developed based on the discrete wavelet transform (DWT) technique where some information has been extracted as the Eigen value of the image and is embedded in the middle-frequency band of the frequency domain. Such embedding has been used for tamper detection and localization.

A novel fragile watermarking scheme based on chaotic system for image authentication or tamper proofing is proposed. The watermark is generated by using pixel values as input values of a chaotic system, and a secret key controls a set of parameters of the chaotic system. A quantization function is introduced to embed and detect water marks. 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 in a way that is difficult to remove. It’s providing copyright protection for intellectual method that’s in digital format. Digital watermarking is an important branch of the information hiding technology. In recent years as digital information is circulating through the world by means of the rapid and extensive growth in internet technology, therefore there is a need to develop newer techniques to protect copyright, ownership and content integrity of digital media. Digital Watermarking technology allow users to embed digital information into audio, images, video and printed materials in a way that is persistent, imperceptible and easily detected by computers and digital devices, shown in figure 1.1.
Digital watermarking is a promising solution for copyright protection, it promises extra robustness n embedded information. The embedded information is called watermarks. The embedded information is called watermarks. We have used a digital watermark which is transparent, invisible information pattern that is inserted into a suitable component of the data source (image) by using a specific computer algorithm.

(b) Properties of digital watermarking

Imperceptibility: The difference between the original image and the watermarked image should be unknown to the human observer.

Trustworthiness: A watermarking scheme should guarantee that it is impossible to generate counterfeit watermarks and should provide trustworthy evidence to protect the rightful ownership.

Robustness: Watermarks should be robust to common signal processing and intentional attacks. The watermarks should still be extracted from the attacked watermarked image.

Security: unauthorized parties should not be able to read or alter the watermark.

Using wavelet transform in the digital image processing has gained popularity in recent times. One of the most popular applications of discrete wavelet transform is in the JPEG2000 image compression scheme whereas its predecessor JPEG standard was DCT based. Discrete wavelet transform is also being used in the domain of digital watermarking. Kundur and Hatzinakos proposed a fragile watermarking scheme for tamper proofing, where the watermark is embedded by quantizing the DWT coefficients. One of the main advantages of using DWT is its power in multi-resolution analysis. This capacity was exploited in the proposed scheme to encode a low resolution version of the image and embed it in the original image. Spread spectrum watermarking method has been a popular choice for watermarking digital media with the purpose of protecting owner’s copyright. However, it was found empirically that for authentication purpose quantization based watermarking performs better than spread spectrum watermarking.

This paper proposes a novel method for authentication of grayscale 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 pixels of an image. To embed the watermark, mid frequency bands of a second level DWT transform was used to ensure both the fidelity of watermarked image and the accuracy of tamper 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 ensure a better balance between the fidelity of watermarked image and the quality of reconstructed image.

II. BACKGROUND

Veyesal Aslantas 2008 presented an optimal watermarking scheme based on singular-value decomposition (SVD) using genetic algorithm (GA). The singular values (SVs) of the host image are modified by multiple scaling factors to embed the watermark image. Modifications are optimized using GA to obtain the highest possible robustness without losing the transparency. Experimental results showed both the significant improvement in transparency and the robustness under attacks. Based on existing experiences to evaluate the applicability of robust watermarking, it is generally agreed that three parameters or requirements, including the quality of watermarked contents, the survivability of extracted watermark after deliberate or unintentional attacks, and the number of bits embedded, need to be considered. However, performances relating 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 requirements into consideration, and add the flexibility to meet the specific design in implementation. With the aid of genetic algorithm, they designed an applicable system that would obtain the good quality, acceptable survivability, and reasonable capacity after watermarking. Simulation results presented the effectiveness in practical implementation and possible application of the proposed algorithm.

Zorana Bankovic 2009 demonstrated the effectiveness of using GA’s in fast searching of the space of the possible solutions. A high detection rate was achieved after a relatively short period of training time. Also the retraining, the system becomes highly adaptable. As the GA’s are inherently parallel in operation there is a possibility of using reconfigurable hardware with the implementation cost much lower. At the same time GA’s can search the solution space in multiple directions at once.

Sanjeev Kumar 2009 presented a digital watermarking algorithm in discrete wavelet transform (DWT) domain for stereo image coding. First, a disparity-image was computed from 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 host image was degraded using Arnold transform. Finally, real coded genetic algorithm (RCGA) was used to estimate the optimal order of Arnold transform and the strength of watermark to fulfill the tasks of security, invisibility and robustness 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 stereo-
pair. Experimental results were presented to evaluate the performance of proposed algorithm in terms of accuracy and robustness.

Chih-Chin Lai 2009 presented a robust digital image watermarking scheme based on singular value decomposition (SVD) and micro-genetic algorithm (micro-GA). In an SVD-based watermarking scheme, the singular values of the cover image are modified by considering multiple scaling factors to embed the watermark image. Determining the proper values of scaling factors is not an easy task. They viewed it as an optimization problem and apply the micro-GA to efficiently obtain the values. Experimental results showed that the proposed approach has good performance against several attacks.

Chen Yongqiang 2009 presented a DWT domain image watermarking scheme to meet the watermarking properties: security, imperceptibility and robustness. In the scheme, watermark comes from a meaningful binary image encrypted by two-dimensional chaotic stream encryption that has more security. In the procedure of watermark embedding, the watermark is embedded into host image through selecting and modifying 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 extracted watermark, Synergetic Neural Network is used in the watermarking identification to overcome the limitation of correlation analysis or the human sense organ after some attacks. The results of their scheme realization and robust experiments showed that the scheme has preferable performance.

Jiann-Shu Lee 2009 proposed a watermarking algorithm for uncompressed video based on Quantization Index Modulation (QIM) and differential energy. The Differential Energy Watermarking (DEW) algorithm has been demonstrated as an effective video watermarking algorithm; while in some scenarios, DEW algorithm cannot provide enough robustness and fidelity. This problem has been solved by above authors. The experimental results indicated that the proposed algorithm is more robust than original DEW and modified low-frequency DEW for lossy compression and transcoding, while maintaining high fidelity.

III. PROPOSED METHOD

(a) Integer wavelet transform

Discrete Wavelet Transform (DWT) is suitable for identifying the areas of the cover image where a watermark can be imperceptibly embedded because of its excellent SPATIO frequency localization properties.

The integer wavelet transform is a specialized version of general DWT which maps integers to integers. The advantage of using integer wavelet transform is that it can be implemented with only fundamental arithmetic operations. In integer wavelet transform, the image is first decomposed in 4 sub bands, LL1, HL1, LH1 and HH1 respectively.

The LL1 band is further decomposed into four sub bands obtaining LL2, HL2, LH2 and HH2. This level wise decomposition can be performed as many times as required. The LL band, or more specifically LL k band of DWT contains the low frequency components of the image and it can be treated as an approximation of the image. Here k indicates the maximum level of decomposition done on the image. Most of the energy of the image is concentrated in this band. Any modification done to this band is visually most perceptible. The HL and LH band of DWT contains horizontal and vertical components of the image and the HH band is called the diagonal band. These latter three bands are high frequency bands. These bands contain the detail information of an image like the edge information. The following figure depicts a two level decomposition of an image using integer wavelet transform.

![Figure 2: Different bands in wavelet transform](image)

(b) Proposed method Analysis

In the proposed method, the HL2 and LH2 bands were used to embed a watermark to the image. Any or both of the bands could be used for embedding the watermark. However, in the proposed method both of
the bands were used to reduce the 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 information of the image. The LL1 component was also used in the proposed scheme as an approximation of the original image and it is encoded into the LSBs of watermarked image as a recovery mark. This recovery mark is extracted from the transmitted image. If any tampering is detected in the transmitted image then this extracted recovery mark is used to restore the image to its original state. To obtain wavelet transform band we used Haar wavelet with lifting scheme. Furthermore, the operation is done in only integer domain to ensure lossless decomposition. It also ensured high computational speed of the proposed scheme.

In the proposed method DWT coefficients of HL2 and LH2 bands were quantized. The technique used for quantizing the DWT coefficients is as follows: Let $d$ is the amount of modulation in DWT coefficient after quantization and $b$ is the value of the watermark bit in the reference pattern that will be embedded. Also, let $p$ is the DWT coefficient to be modulated and $m$ is the modulated DWT coefficient. Now, $m$ will be modulated using following algorithm:

1. $f = \text{floor}(p/(2*d))$
2. $c = \text{ceil}(p/(2*d))$
3. if $|v-f| <= |v-c|$
   1. if $b == 0$
      1. $m = f*2*d$
   2. else
      1. $m = f*2*d + d$
5. else
   1. if $b == 0$
      1. $m = (f+1)*2*d$
   2. else
      1. $m = (f+1)*2*d + d$
7. end

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

1. Divide the image into $8 \times 8$ sub blocks
2. Compute 2-level DWT for each of the block
3. LL1 band of a block $X$ is embedded into the LSB of a different block $Y$ as a recovery mark. The location of block $Y$ is determined by using a secret watermark key which should be available to the watermark detector.
4. Modify the DWT coefficients of the HL2 and LH2 band according to the algorithm described above. Each bit of the watermark image is embedded in one coefficient of HL2 band and in one coefficient of LH2 band
5. Compute Inverse DWT for each block to get the watermarked image

Let $x$ is a DWT coefficient of received image. Then, watermark bit $b$ from this coefficient was extracted using the following algorithm:

1. Divide the image into $8 \times 8$ 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 HL2 and LH2 band of each of the block of the image
5. Compute correlation coefficient of extracted watermark and original watermark for each block
6. If the correlation between extracted watermark and original watermark is larger than the threshold then mark the block as authentic, otherwise mark the block as inauthentic or tampered.
7. Replace the tampered blocks using recovery mark
IV. 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
V. CONCLUSION
The proposed method is computationally fast as it uses only integer based operation. Watermarked image in the proposed 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 proposed algorithm and the quality of the recovered image was also quite satisfactory. Proposed method ensured a better balance between the fidelity of watermarked image and the quality of the recovered image as compared to the method proposed

REFERENCES