UNIQUE APPROACH TO WATERMARK JPEG 2000 IMAGES

Suraj G. Nair, Kartik A. Gupta, MandarPatil, SiddheshGawde, Miss. RajashreeGadhave.

ATHARVA COLLEGE OF ENGINEERING
MALAD (WEST), INDIA
surajnair921992@outlook.com
kartikgupta11120@gmail.com
mpatil00123@gmail.com
sidgwd@gmail.com
rajashree86@gmail.com

***Abstract*— Digital media content is often distributed in compressed and encrypted format in the networking environment. These digital media is vulnerable to many violations such as illegal copying, tampering and destroying authority of the digital media so as to use them illegally. Hence it becomes necessary to watermark these compressed encrypted media items in the compressed-encrypted domain itself for tamper detection or ownership declaration or copyright management purposes. It is a difficult work to watermark these compressed encrypted media content as the compression process would have packed the information of raw media into a less number of bits and encryption would have randomized the compressed bit stream. Watermarking such a randomized bit stream can cause a serious degradation to the quality of the digital media. The method that we use is both secure and will allow watermarking in a predictable manner in the compressed encrypted domain. In this paper, we propose analgorithm to watermark JPEG2000 compressed and encrypted images.**

Keywords— **Compressed and encrypted domain watermarking, retrieval of watermarking.**

I. INTRODUCTION

In the last two decades one of the greatest technological events was of the invasion of digital media into everyday life aspects. Digital media can be stored efficiently and that also with a very high quality, and the data can be manipulated very easily using computers and various software's available. Further, the digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality of the digital data during transmission.Digital media has numerous advantages over analog media. The quality of digital audio, digital images and digital video signals are better than that of their analog media signals. Editing has become easy because anyone can access the exact discrete locations that need to be changed in the digital media. Copying has also become simple with no loss of fidelity and a copy of a digital media is identical to the original. With the distribution of digital multimedia all over the World Wide Web, the Intellectual Property Right i.e. (IPR) are more threatened than ever due to the possibility of unlimited copying of digital media. One solution for protecting from this situation would be to restrict access to the digital data using some encryption techniques. However encryption does not provide overall protection to the digital media from such problems. Once the decryption of encrypted digital data is done, they can be freely distributed or manipulated over the World Wide Web. The above problem can only be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the authenticity of image or ownership. Watermarking is an active method to prevent any kind of image forgery or manipulation of digital data. It is derived from an older technique known as steganography. A technique for concealed communication between two parties over a network is called steganography. In this method, a secret message is hidden within another unrelated message and then communicated to the other party over the network. As opposed to this in watermarking technique, again one message is hidden in another and then communicated over the network, but here in this technique the two messages are related to each other in some way. Steganography methods are in general not a robust technique. But in watermarking technique, as opposed to steganography, there is the additional advantage of being a robust technique against number of attacks. It is difficult for an attacker to destroy the embedded watermark in the digital media, even if the existence of the hidden information in the digital media content about the ownership or authentication is known and even if the algorithmic principle of the watermarking method used is public. The structure of paper is as follows in section 2 we have reviewed the work which is already done in the field of watermarking of images. In section 3 we propose a robust method to watermarking images in compressed and encrypted domain and also retrieving the watermark. In section 4 we describe the application areas where the proposed technique can be applied followed by section 5 consisting the conclusion.

II. RELATED WORK

The earliest work in the field of reversible data embedding is the Barton patent, in 1994. In this patent, the bits were first

compressed and then added to the bit strings which were to be overlaid, after which these bits will then be embedded into the data block. In order to losslessly recover the original image, Honsinger, et al[2] reconstructed the payload and then subtracted the payload from the embedded image.In their method, Schyndel, Tirkel, and Osborne [11] generated a watermark using an m-sequence generator. Here the watermark was either embedded or added to the least significant bit (LSB) of the original image to produce the watermarked image. The extraction of watermark from a suspected Image was done by taking the least significant bits at the proper locations. Detection wasdone by cross-correlation of the original and extracted watermark. Schyndel et al showed that the resultant image contained an invisible watermark with extractionprocedures which were simple. However, the watermark was not robust to additive noise.In their work Cox et al. [12] noted that in order for a watermark to be robust, watermark should be placed in perceptually significant areas of the image. Here the watermark was based on 1000 random samples of a N (0,1) distribution. These 100 random samples were added to the 1000 largest discrete cosine transform (DCT) coefficients of the original image, and the inverse of the DCT was taken to retrieve the watermarked Image. For detection purpose, the watermark was extracted from the DCT of the image which is under suspicion. Here, extraction was based on knowledge of the original signal and the exact frequency locations of the watermark. Now the correlation coefficient was computed and set to a threshold such that if the correlation was large enough, then the watermark was detected. This method was robust to image scaling, cropping, JPEG coding, dithering, and rescanning.Here we will see the work of Xia, Boncelet, and Arce [13] who proposed a watermarking scheme based on the DWT which is theDiscrete Wavelet Transform. The watermark was modelled as Gaussian noise. This watermark was added to the middle and high frequency bands of the image to be watermarked. The process of decoding consisted of taking the DWT of a potentially marked image. Sections of the watermark from the image were extracted and these sections were then correlated with sections of the original watermark. If the cross-correlation came above a threshold, then the watermark is detected otherwise the image was again decomposed into finer and finer bands until the extracted watermark was correlated with the original watermark. This technique was more robust than the discrete cosine transform method [12]. After embedding zero-tree wavelet compression and half-toning were performed on the watermarked images.Improvements on the above watermarking scheme were possible by using the properties of theHuman Visual System. Bartolini et al. [14] firstly generated a watermarked image from DCT coefficients, then by performing spatial masking on the new image the Watermark was hidden. Kundur and Hatzinakos [15] embedded the watermark in the image in the wavelet domain. Here the strength of the watermark was decided by the contrast sensitivity of the original image. Both the techniques showed resistance to common signal processing operations.Based on the Human Visual System, Delaigle et al. [16] proposed a unique watermarking scheme based. In this method, firstly binary m-sequences were generated and then modulated on a random carrier. This image served as the watermark is then masked based upon the contrast between the original signal and the modulated image. The masked watermark is then embedded to the original image to form the watermarked image. This method was robust to JPEG coding, additive noise and rescanning Craver et al [17] noted that certain methods of watermarking an image were affected by counterfeit attacks. They also showed that the method proposed by Cox et al. could be attacked by creating both original image and watermark which are faked and that cannot be distinguished from the true original image and watermark. To prevent this kind of attacks, they modified the algorithm of Cox et al. by making the watermark dependent on the original image. This new method was less affected by counterfeiting and also maintained robustness. A watermarking system was developed by Bas, Chassery, and Davoine [18] using fractal codes. A collage map was derived from 8x8 blocks of the original image and from the Discrete cosine transform (DCT) of the image. Here watermark was added to the collage map which produced a marked image. The results showed that performance of fractal coding in the DCT domain was better than coding in the spatial domain. The DCT-based watermarking technique proved to be robust to JPEG compression meanwhile spatial fractal coding produced block artifactsafter compression. An extension to the patchwork algorithm for achieving reversible data embedding was proposed by Macq[3]. A reversible data-embedding technique withhigh capacity was developed by Fridrich, et al.[4], based on embedding message on bits in the status of group of pixels.Two reversible data-embedding techniques for loss image format JPEG was also described by them. Some theoretical capacity limits of lossless data compression was provided by Kalker, et al.[5], based on reversible data embedding and give a practical code construction. A high capacity, low distortion reversible data-embedding algorithm was presented by Celik, et al.[6], by compressing quantization residues. In the past few years different techniques of reversible watermarking had been proposed which by losslessly compressing these bits used to remove bits from block of the image and then to provide the space for the watermark to be embedded in the same block.An algorithm was proposed by Tian using difference expansion and using Haar wavelet transform. Here in this method, it chooses the expandable coefficients and then embeds an extra bit into these coefficients. The watermarked image thus formed in the method is imperceptible and exact recovery of watermark is also possible.But here in this method the embedding capacity is less. An algorithm proposed by Alattar which uses difference expansion of a generalized integer wavelet transform there by embedding a set of watermark bits in a vector of pixels.

III. PROPOSED SYSTEM

Digital watermarking is similar to watermarking physical objects except that it hides information, for example a number or text, in digital media, such as images, video or

audio. In digital watermarking a low-energy signal is unnoticeably embedded in another signal. The low energy signal or the embedded signal is called watermark and it represents some security or rights information about the main signal. The signal in which the watermark is embedded is called as cover signal since the watermark is covered by it. The watermark is embedded in the cover signal in which the cover signal can be can be a still image, an audio clip, video sequence or a text document which is in digital format. The digital watermarking system mainly consists of 2 parts a watermark embedder and a watermark detector as shown in Fig 1. The watermark embedder embeds a watermark onto the cover signal using a key and the watermark detector on the other hand detects the presence of watermark signal using the key.

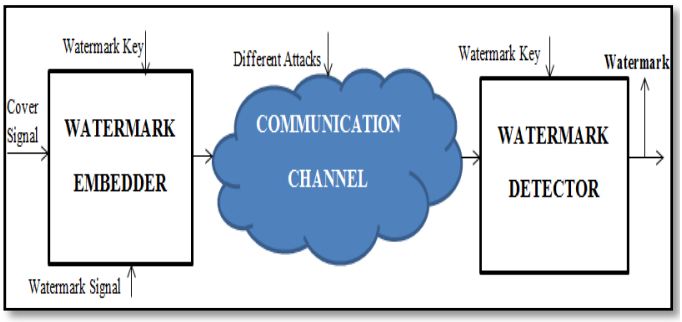

Fig. 1 Digital Watermarking System

A unique watermark key exists for every watermark signal (i.e., it has a one-to-one correspondence with watermark signal). The watermark key ensures that only authorized parties can detect the watermark and hence is private and known to only authorized parties. Further, the communication channel can be prone to security attacks (i.e., noisy and hostile) and hence the digital watermarking techniques should be resilient to both noise and security attacks.

The architecture is divided into 2 parts consisting of Watermark embedding as shown in Fig 2 and Watermark extraction as shown in Fig 3. In the first part we have the image encoder which encrypts the image. Then we insert the watermark bits into the image.

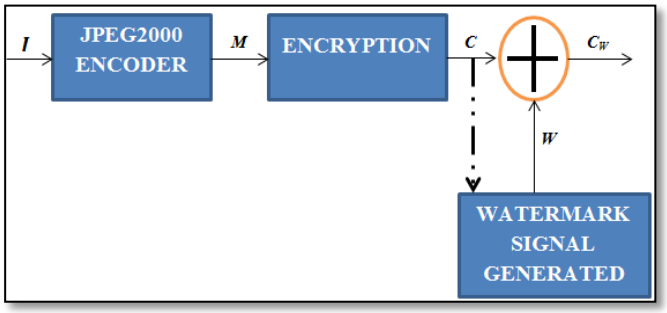

Fig. 2 Watermark embedding.

In the second part the image is decrypted and then the watermark bits are extracted.

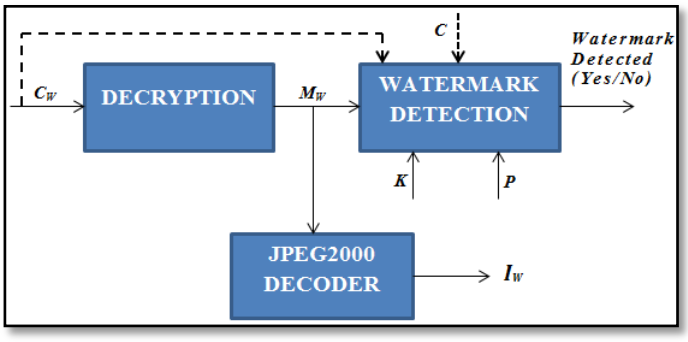

Fig. 3 Watermark extraction

This system shows a method for a colour digital image to carry 'hidden' encrypted information with it. In standard, any cipher that are uniformly distributed and consisting of floating point numbers can be used to perform this. The scheme can be used to make certificates documents, and other image based data self authenticating. If the snooper catches the information being sent, give him the idea that the information being sent if of value and he might try to decrypt it , thus it is one of the weaknesses of all encryption systems. The key solution of this problem is to make sure that the information is encrypted using a strong encryption technique and some message is hidden inside the document being transmitted which later on helps in claiming the authenticity of the document by its original owners. The above approach makes sure that the cipher text gives the intruder a tough challenge in decrypting the information sent, even if decrypted the information still will be authenticated. We will be working on the different modules to accomplish the task.
The different modules that we would be working upon are:

A. Watermarking Domains

1) Watermarking in compressed form: Many methods have been proposed which focus on the robustness to compression and some claimed that their algorithms are robust to JPEG compression. These algorithms usually use normalized correlation as the measurement to detect the existence of the watermark information that is not suitable for data hiding. Once encrypted, it cannot be decompressed at any intermediate level. In this domain, even a slight change in the compressed information might result in a large amount of decline in image quality. Therefore the position to embed a watermark in a compressed image should be selected with precaution so that the reduction in the image quality can be minimized.

2) Watermarking and Its Retrieval: Once the compressed encrypted content is received by the distributor, it should be possible to embed watermark without decrypting. This is required to preserve confidentiality of content and secure it from different attacks of decrypting the cipher. In this domain, modifying an individual bit in encrypted information may result in random decryption of it. Therefore encryption has to be selected so that image quality can be maintained by minimizing the deformity due to embedding. Also, as encryption may lead to cipher text expansion the gain in

compression should not be absent and also one shouldn't be able to copy the images as it becomes hard to find the exact watermark from the cipher text in the embedding procedure.

B. Steps of Compressing JPEG2000

1. The first step involves an input image which is divided into rectangular, non-overlapping tiles. With respect to a high-resolution grid components are tilled with different sub-sampling factors
2. Size of each tile is maintained to be the same except the tiles around the borders of the image. The input series are converted into high-pass & low-pass coefficient series using DWT.
3. The wavelength coefficient containing a fixed dead zone are uniformly quantized about the origin
4. Each coefficient's magnitude is divided by quantization step size and rounding down
5. Using packet partition each sub-band is divided into regular non-overlapping rectangles
6. A packet partition location comprises of three spatially consistent rectangles
7. To obtain code blocks each packet partition location is divided into non-overlapping rectangles
8. In the final stage entropy coding is carried out and each code block is collected and arranged to form the body of the packet.

C. Watermarking Schemes

1) Spread Spectrum (SS)- Many different watermarking techniques for images and video has been proposed. Mostof them are based on ideas derived from spread spectrum radio communications,[19] namely additive embedding of asignal which is(adaptive or non-adaptive) pseudo-noise watermark pattern, and recovery of watermark by correlation.The watermark signal is generated without using host data for spread spectrum.

2) Scalar Costa Scheme- It is a suboptimal technique using scalar embedding and reception functions. SCS scheme for watermark embedding was proposed by Eggers et al.

3) Rational Dither Modulation- It is a data-hiding technique which is quantization-based, that is basically responsible to amplitude scaling's and modifies it in such a way that the result becomes invariant i.e.never changingto realize attack [20]. It is for the intention of detecting the bit error rate and to study trade-off between the qualities against payload capacity. These schemes mentioned above for retrieval or destruction of the watermark of an image can operate either in compressed encrypted or decrypted domain. Since detecting watermark for claim verification of image, copyright breach detection or traitor tracing, can be done easily, the attacks are considered in compressed domain as the information is distributed and copied often.

D. Data Embedding

Embedding a large amount of secret data into grey level and colour images with low warping has become an important issue. Proposed method can provide high data capacity with acceptable digital image quality. In this stage, the payload capacity average against bit planes numbers watermarked under various resolutions using Scalar Costa scheme. The payload capacity average is determined as the proportion of average number of embedded bits to average of compressed stream size format, where average is calculated as a plain mean. Increase in amount of greater resolutions dimensions, results in increase in payload capacity, generating additional compressed bytes, allowing extra embedding space.

IV. APPLICATIONS OF THE PROPOSED TECHNIQUE

The proposed digital watermarking technique has wide ranging applications [7,8,9,10]. Some of the applications are enlisted below.

A. Copyright Protection.

Digital watermarks can be used to establish and protect copyright control of a digital media. Digital media content can be embedded with watermarks depicting metadata identifying the original copyright owners of the digital data.

B. Copy Protection.

Digital media data can be watermarked to signify that the data cannot be illegitimately duplicated by anyone else. There are devices which are efficient of identifying replication can then detect such watermarks and prevent unauthorized duplication of the content.

C. Tracking.

Digital watermarks can be used to track the usage of digital media content anywhere. Each copy of digital content can be uniquely watermarked with metadata specifying the original authorized users of the content who can use the image anywhere. Such watermarks can be used to detect illegal replication of content by identifying the users who replicated the content illegally. The watermarking technique used for tracking is called as fingerprinting.

D. Tamper Proofing.

Digital watermarks, which are feeble in nature, can be used for tamper proofing of the digital media content. Digital content can be embedded with watermarks which are fragile that get destroyed whenever any sort of change is made to the content. Such watermarks can be used to authenticate the content. The purpose of this application is to detect alterations and modifications in a document. The three pictures below illustrate an example of this application.

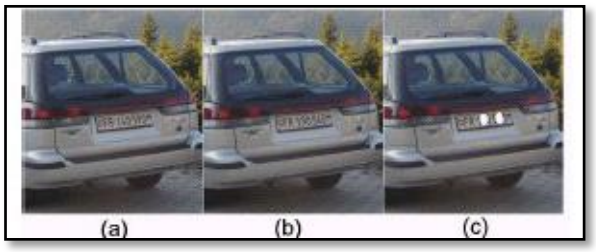

Fig. 4(a,b,c) Tamper proofing.

Fig.4a above shows an original image of a car which has been protected with a watermarking technology for tamper proofing. In the centre Fig.4b, the same image is shown but with a small modification i.e. the numbers on the license plate of the car have been changed. The image Fig.4c on the right shows the photo after running the watermark detection program on the tampered image where the tampered areas are indicated in white and we can clearly see that the detected areas in the image correspond to the modifications applied to the original photo.

E. Broadcast Monitoring.

By embedding watermarks into marketing advertisements, the advertisements can be watched carefully whether the advertisements are broadcasted at the appropriate instants by means of an automated system. The system obtains the broadcast and searches these watermarks identifying where and when the advertisement is broadcasted. The same process can also be used for video and sound clips.

F. Covert Communication.

Covert communication is another achievable application of digital watermarking. The watermark embedded in the digital data, which is the secret message, can be embedded to the digital image or video in an indistinguishable way to communicate the valuable information through the content from the sender to the intended receiver while maintaining low probability of interference by other unintended receivers over the network communication.

G. Identity Card / Passport Security.

Information akin to the person in a passport or ID card can also be contained in the person's photo that appears on the ID card. Extracting the embedded information in the image on the passport and comparing it to the written text can verify the ID card. The inclusion of the watermark to the image on passport or ID cards provides an additional level of security in this kind of application. For example if ID card is filched and the person changes the picture on the identity card with another person's picture, the lack of success in extracting the watermark from the image will disqualify the ID card.

H. Medical Safety.

Embedding the important data and patient's name in medical image such as on a patient's identity card could increase the confidently of medical information of the patient as well as the security of that information.

V. CONCLUSION

In this paper we propose a novel technique to embed a robust watermark in the JPEG2000 compressed encrypted images using the watermarking schemes. The algorithm is simple to implement as it is directly performed in the compressed-encrypted domain, i.e., it does not require decrypting or partial decompression of the content. Our technique also preserves the confidentiality of content as the embedding is done on encrypted data.

REFERENCES

[1] M. Rabbani and R. Joshi, "An overview of the JPEG 2000 still image compression standard," Signal Process.: Image Commun., vol. 17, no.1, pp. 2–49, 2002.

[2] Honsinger, C.W., Jones, P., Rabbani, M., and Stoffel, J.C.: 'Lossless recovery of an original image containing embedded data'. US patent no. 6278791, 2001.

[3] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in Proc. EUSIPCO, Sept. 2000, pp. 532–537.

[4] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—new paradigm in digital watermarking," EURASIP J. Appl. Signal Processing, vol. 2002, no. 2, pp. 184–197, Feb. 2002.

[5] T. Kalker and F. M. J. Willems, "Capacity bounds and constructions for reversible data hiding," in Proc. 14th Int. Conf. Digital Signal Processing, vol. 1, July 2002, pp. 70–77.

[6] Celik, M.U., Sharma, G., Tekalp, A.M., and Saber, E.: 'Reversible data hiding'. Proc. ICIP, 2002, vol. 2, pp. 156–160.

[7] AlperKoz, "Digital Watermarking Based on Human Visual System", The Graduate School of Natural and Applied Sciences, The Middle East Technical University, pp 1 – 9, Sep 2002.

[8] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", in AlpVision, Switzerland, pp 1 – 5.

[9] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, "A SURVEY ON WATERMARKING APPLICATION SCENARIOS AND RELATED ATTACKS", IEEE international Conference on Image Processing, Vol. 3, pp. 990 – 994, Oct. 2001.

[10] A White paper on "Digital Watermarking: A Technology Overview", Wipro Technologies, pp. 1 – 8. Aug. 2003.

[11]RSchyndel, A. Tirkel, and C .Osborne, "A Digital Watermark,"Proc.IEEEInt.Conf. on Image Processing, Nov. 1994, vol. II, pp. 85-90.

[12] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1672-1688, Dec. 1997.

[13] X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 547-552.

[14] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing,Oct. 1998, vol. I, pp. 449-455

[15] D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method UsingWavelet-Based Fusion," Proc. IEEE Int. Conf. on Image Processing,Oct.1997,vol.I,pp.543-548.

[16] J. Delaigle, C. De Vleeschouwer, and B. Macq, "Psychovisual Approach to DigitalPicture Watermarking," Journal of Electronic Imaging,vol.7,no.3,pp.627-641,July1998.

[17] S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships withInvisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE Journal on Selected Areas in Communications, vol. 16,no.4,pp.572-587,May1998.

[18] P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images,"Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct.1998,pp.468-474.

[19] R. Dixon, Spread Spectrum Systems, John Wiley & Sons, New York, NY,USA,1984.

[20] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks", IEEE Trans. Signal Process., vol. 53, no. 10, pt. 2, pp.3960–3976, Oct. 2005.

.

