www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5 May, 2014 Page No. 5723-5726

An Implementation of Image Watermarking by Using Gradients

Dnyandevi W.Shrirao, Prof.Sulbha patil, Prof. Sonal Honale
Mtech Student of Computer science Engineering
Computer Science Engineering
Abha College of Engineering
Nagpur, India
radhagulhane@gmail.com
Dean and Prof. in Abha college of engineering
Computer Science Engineering
Abha College of Engineering
Nagpur, India
sulbhapatil@gmail.com
Assistant prof. in Abha College of enggineering
Computer Science Engineering
Abha College of Engineering
Nagpur, India
sonalhonale@gmail.com

***Abstract*—Digital image can be copy from one place to another Place are easily , and our image are distribute from person to person and image easily uploaded on the internet. Images can be appeared widely in the internet and can be copied from the internet. To protect the image applied the watermark. Watermark is method to embed the data into an image. Data must be placed into an actual pixel. Watermarking are two types:1) Visible watermarking and 2) Invisible Watermarking. In proposed system invisible watermarking are used, Because it is more secure as compare to visible watermarking. In this scheme watermark are placed on the gradients vector. This system is more secure as compare to other watermarking scheme . Other scheme are based on coefficient based, hence by using filtering method and compression techniques watermark and image are separated from each other. Proposed system are more secure and in this technique gradient vector are used to embedded the data.**

Keywords-Digital watermarking, watermarks

I. INTRODUCTION

Peoples are showing interest on hiding information like event, particular occasion, or any secret message in an image such that it could be kept safely and also for secret communication. Novel sample-based methods are proposed to hide some information/data bits in the JPEG compressed domain. To protect the image updating the original image by using watermark and to provide the security key such as authentication or copyright code, when embedding data into an actual pixel the original image is unchanged.

Four novel techniques are proposed to add watermarks for different purposes. First one is Single Watermark Embedding (SWE) is use to add a watermark bit sequence using two secret keys in digital images . The second one technique is called as Multiple Watermark Embedding (MWE) extends SWE to add multiple watermarks simultaneously in the same watermark space at the time of minimizing the watermark energy. Third technique is called as Iterative Watermark Embedding (IWE), it adds watermarks in JPEG-compressed images. The proposed iterative approach can minimize at large extent the potential removal of watermarks in the JPEG recompression process. And the fourth technique is called Direct JPEG Watermark Embedding (DJWE), it is an extension of the IWE. DJWE adds thewatermarks with less computation complexity then IWE and uses the Human Visual System (HVS) model to alter the prioritization of the coefficient to achieve good visual quality.

The major technical problem is to develop a highly robust digital watermarking technique is by using the different filtering and compression method watermark and image are separated from each other.

The proposed system used the algorithm of

II. METHODS OF IMAGE WATERMARKING

I. J-Mark

Method for watermarking called J-Mark is proposed to add secret information in JPEG compressed domain. To add the data, Quantized DC and AC coefficients

are selected. The J-Mark is the extension of the previously proposed method called DC-Hide .To adds data in AC coefficients, there are two problem which arises. The first problem is the quantization factors for AC coefficients which are usually large, and thus even a slight change on quantization AC coefficients may affect significantly the visual quality of the image. The second problem is the modification on AC coefficients, it affects the identification of texture blocks at the decoder since the texture blocks are selected based on the energy of the AC coefficients. To resolve the above problems, solutions are proposed called J-Mark which is used to hide data in JPEG images with negligible visual degradation. J-Mark adds hidden data into a JPEG compressed image resulting in another JPEG image with the hidden data.

There are steps which are involved in J-Mark: block selection, DCT coefficient selection and the modification of the selected DCT coefficients of the selected blocks. Alternatively, J-Mark operates on an uncompressed image by compressing it with JPEG with the quantization table and target quality factor. The output JPEG image from J-Mark is not going to be transcoded or processed further before the hidden data are extracted. We can say that it is assumed that there are no hostile attacks or casual signal processing on the JPEG compressed image. Under such assumption, the hidden data can be extracted with better perfection.The data hidingprocess of J-Mark is shown in Figure 1 and the data extraction is shown in Figure 2.

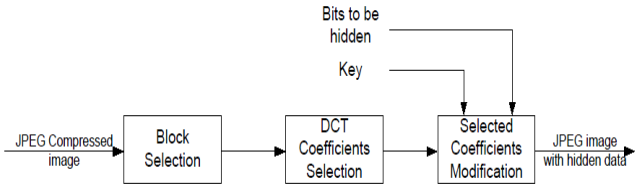


Figure 1: Data hiding process of J-Mark

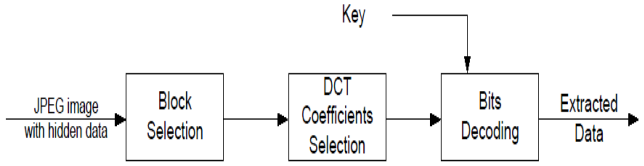


Figure 2: Data extraction process of J-Mark

II. Single Watermark Embedding (SWE)

A vector-based watermarking technique is proposed called as Single Watermark Embedding (SWE). SWE can be used to add a single watermark in an image and the added watermark is represented by a bit sequence. In general, the proposed SWE can also be used for data hiding. SWE can be applied in transform domains such as DCT, and possibly the spatial domain, of an image. Some of the selected image pixels or transform coefficients are grouped together to form a vector and are called as watermark host vector. The watermark host vector is divided into two vectors i.e. disjoint sub-vectors and each sub-vector is used to add one bit information.

Let the watermark host vector be [ ] M Y y , y ,..., y 1 2 = with length M. The watermark, [ ] N L l ,l ,...,l 1 2 = with ∈{0,1} i l , is a bit sequence with length N where N<<M. The bit sequence may be a meaningful image such as information of the image owner or the information related to the logo of the host images such as the owner's name, image ID, … etc. The watermark is modulated by a bit-wise logical XOR operation with a pseudo-random bit sequence [ ] N S s ,s ,...,s 1 2 = with ∈{0,1} i s to give the modulated watermark sequence [ ] N W w ,w ,...,w 1 2 = with i ii w = s ⊕l.Through this design, electric meter will communicate with base station node and will send utility data such as unit count and receive bill for that unit count. In this way, it is convenient to get the data wirelessly from consumer side. This system consumes low power to set the network.

Symbol	Description
$\boldsymbol{Y} = y , y ,..., y_M$	Watermark host vector
$\boldsymbol{Y} = y_{i1}, y_{i2},..., y_{ip}$	i^{th} sub-vector of $\boldsymbol{Y}$
M	Length of host vector
N	Length of bit sequence
P	Length of sub-vector
$\boldsymbol{W} = w1 , w2 ,..., w_N$	Modulated watermark bit sequence
$\boldsymbol{W'} = w1 ' w2, ' ,..., w_N'$	Decoded watermark bit sequence

Table 1: List of Symbols in SWE

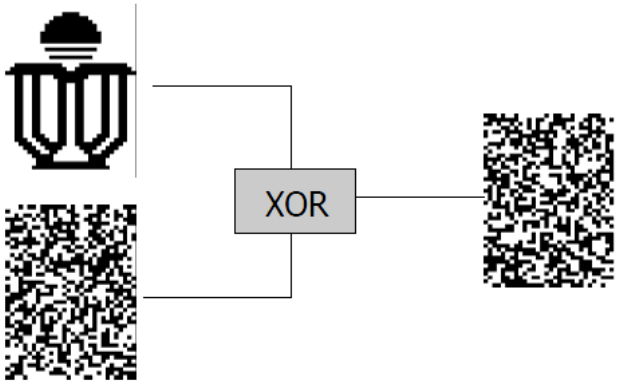


Figure 3: Modulation of Watermark

III. ROBUST IMAGE WATERMARKING BY USING GRADIENT VECTORS

Gradient direction watermarking (GDWM) is based on the uniform quantization of the direction of gradient vectors. In this method, the watermark bits are embedded by

significant gradient vectors at multiple wavelet scales. GDWM has the following advantages:
1) Increased invisibility of the embedded watermark because the watermark is embedded in significant gradient vectors,
2) Robustness to amplitude scaling attacks because the watermark is embedded in the angles of the gradient vectors, and,
3) Increased watermarking capacity as the scheme uses multiple-scale embedding. The gradient vector at a pixel isdeclared in terms of the discrete wavelet transform (DWT) coefficients. To quantize the gradient direction, the DWT coefficients are varied based on the derived relationship between the changes in the coefficients and the change in the gradient direction. It is shown in the experimental results that the proposed GDWM performs well as compared to other watermarking methods and is robust to a wide range of attacks, e.g., Gaussian filtering, amplitude scaling, median filtering, sharpening, JPEG compression, Gaussian noise, salt & pepper noise, and scaling.

To quantize the gradient direction, we propose the quantization index modulation; QIM solves the problem of angle discontinuity at by quantizing the absolute angle value. To quantize the gradient angle, we first derive the relationship between the gradient angle and the DWT coefficients. The corresponding DWT coefficients are then modified based
on the changes introduced by quantizing the gradient angles. Thus, to embed the watermark bits, the gradient field that corresponds to each wavelet scale is obtained.

The straightforward way to insert the watermark bits is to partition the gradient fields into non overlapping blocks. Each watermark bit is then embedded in each block. The bit is inserted into the most significant gradient vectors of the block. Embedding the watermark in the significant vectors makes it robust to attacks. In natural images, however, some parts of the image may have all or most of the significant vectors, while other parts may have none.

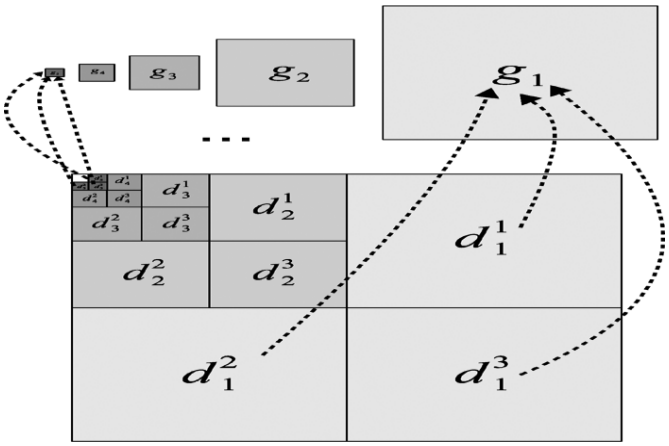
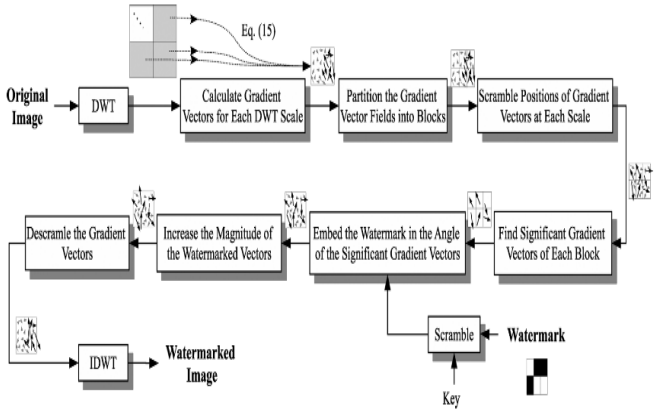


Figure 4: Illustration of five-level gradient field, obtained from five-level wavelet decomposition.

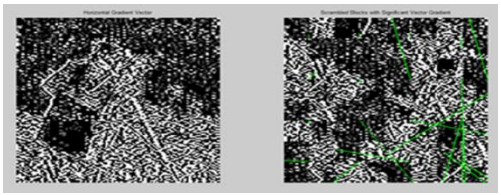
To achieve high fidelity-robustness trade-off, HVS models could be employed in watermark embedding. Towardsthis aim, the *just noticeable difference* (JND) can be obtained for each transform-domain coefficient. [1]



IV.EXPERIMENTAL RESULTS

In proposed system image is decomposed into horizontal plane, vertical plane, diagonal plane and approximate plane & apply the DWT on the original image and then calculate the gradient vector of each scale, partition the gradient vector field into block and scrambling the position of gradients vectors at each scale for the security purpose. The results of image decomposition and Calculating gradients vector and scrambling the position of gradients vector are shown in the following fig(a), (b), (c).

(a) Original Image(b) Image decomposition in approximate, vertical, horizontal, diagonal plane.



(b) Calculate Gradients and scrambling the Gradient vectors

V .CONCLUSION

The most important property of any watermarking technique is its robustness to various attacks and capability to preserve the data hidden. Out of the mentioned techniques the multiscale gradient direction is the most robust method that can be employed to any secured watermarking method but has more complexity and requires a lot of computation. Proposed method inserts the watermark bit in the direction of significant gradient vector so it is more secure.

REFERENCES

[1] Ehsan Nezhadarya,, Z. Jane Wang, and RababKreidiehWard, "A Robust image watermarking based on multiscale gradient direction quantization" IEEE Trans. Information Forensics and security, Vol 6, No. 4, Dec 2011

[2] Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom" Watermarking applications and their propertiesPublished in the Int. Conf. on Information Technology'2000.

[3] L.Ghouti, A.Bouridne, M.K.Ibrahim, and S.Boussakta, "Digital image watermarking using balanced multiwavelets," IEEE Trans.Signal Process., vol. 54, no. 4, pp. 1519–1536, Apr. 2006.

[4] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," Proc. IEEE, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[5] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001

[6] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," IEEE Trans. SignalProcess., vol. 51, no. 4, pp. 1118–1123, Apr. 2003.

[7] H. W. Lin, S. Q.Yang, watermark algorithm for color image authentication and restoration, in proceedings of IEEE International conference on Electronic and Mechanical Engineering and Information Technology, pp. 2773-2776,2011

[8] K. Xiao Jun, D. Li Jun, A digital watermarking algorithm based on image segmentation and DFT, in Proceedings of IEEE international conference on Information science and Engineering, pp.1511-1514,2009

[9] J.Sang. M.S.Alam, Fragility and robustness of binary phase only filter based fragile/semi fragile digital image watermarking. IEEE Trans. Insturm. Megas.57 (3), 595-606(2008)

[10] Y.S. Chen,R.Z. Wang, Reversible authentication and cross recovery of image using (t, n) threshold and modified RCM watermarking, in IEEE International conference on Intelligent Information hiding and Multimedia signal Processing. Germany, pp.47-50, Oct 2010