CAM-based Digital Image Watermarking Revisited

Mohamed Tahar Ben Othman, Senior Member, IEEE
Computer Science Dept., College of Computer,
Qassim University,
KINGDOM of SAUDI ARABIA
Emails: maathaman@qu.edu.sa; mtothman@gmail.com

Abstract: The Content Addressable Method (CAM) is used in a new RGB image watermarking system. The image is divided into clusters indexed by CAM technique. Each cluster holds part of the watermark in sequence. A cluster is segmented into equal portions each of them is used to duplicate a number of bits of the watermark. These portions are numerated by a counter added to some LSB bits of the pixels. We used two techniques for this segmentation. In the first technique, the cluster's pixels are allocated to a portion in a first visited first allocated FVFA way. The counter is added to portions in sequence. In second technique, a Content Based Counter CBC is used to allocate pixels to the portion and a uniform redistribution is made for each cluster. The redistribution is done in a way to minimize the modifications in counter space. Both techniques show robustness resisting to rotation attacks. The CBC performs better as it minimizes the Number of Bit Change Rate (NBCR) in the counter field. Using CBC our watermarking system resists better to cropping attacks.

Key-Words: watermarking, image rotation, clustering, color images, Content Addressable Method, Content Based Counter.

1 Introduction

Several watermarking systems have been proposed for digital image protection. On the other hand, the large number of attacks which appear as fast as new algorithms are proposed emphasizes the limits of these latter. The need of image watermarking is growing for different aspects among which: data privacy, image integrity, authenticity, tamper detection and image correction, and confidentiality. Images can be tampered either by accidental or intentional attacks. To preserve the aforementioned aspects, intensive researches were conducted in the last decade. Image watermark is widely used for such purpose.

Digital image watermarking is different from steganography which in its turn different from Cryptography. Cryptography is defined as the art and science of secret writing. The word comes from Greek where the words kruptos and graphen mean secret and writing, respectively. The focus in cryptography is to protect the content of the message and to keep it secure from unintended audiences. On the other hand, steganography is the art and science of hiding information in ways that prevent the detection of hidden messages. Steganography literally means “covered writing” and is usually interpreted to mean hiding information in other information. Comparing it to cryptography, steganography has its advantage because the message itself will not attract the audiences, as the very nature of a steganography system is to hide the message in an imperceptible manner. Watermarking is the process of embedding a message on a host signal. Watermarking, as opposed to steganography, has the additional requirement of robustness against possible attacks. Fig. 1 presents the general watermarking system.

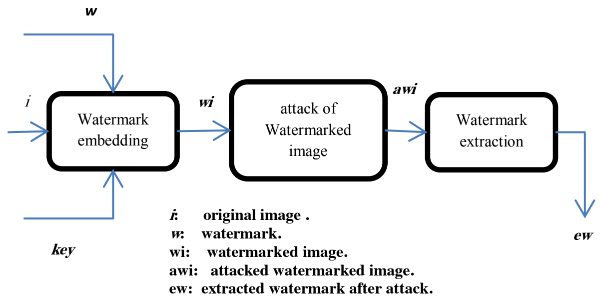


Fig. 1: General watermarking system

There are two main watermarking domains namely spatial and frequency domain [14]. In spatial domain techniques the watermark is embedded directly into the pixel data. In frequency domain techniques a transformation of the image to the frequency domain is made first using transforms such as SVD, DCT, DFT, or DWT. The watermark is embedded to the frequency domain coefficients and then the inverse transform is performed to restore the watermarked image. Several techniques were used for image watermarking and used to maintain a certain level of some aspects mentioned above among these techniques are: Matrix Norm Quantization [1,2], Hamming Codes [3], Singular Value Decomposition watermarking [4,5], DFT [5,6], Arnold Scrambling [7], Dual-Tree wavelet transform (DWT) [5,8], Discrete Cosine Transform (DCT) [8]. Some solutions mixed both spatial and frequency domains [16] to get better results. Several papers discussed the open research issues like in [17-31]. Our work is spatial watermarking technique based on image clustering using the Content Addressable Method (CAM). Each cluster contains all pixels of the image which have the same content address provided by the CAM technique.

The rest of this paper will be as follows: A review of the related works is presented in Section 2. Introduction to watermarking domains is presented in Section 3. The proposed System is given in Section 4. Section 5 shows the different experiments results, followed by a conclusion and future directions in Section 6.

2 Related works

In this section, we will give a brief study of some researches that used clustering in their watermark system. Lingling *et al* used in [9] the Statistical Quantity Histogram (SQH) shifting and clustering to construct a new watermark system for good robustness and low run-time complexity. They obtained comprehensive performance in terms of reversibility and robustness. Their work focused mainly on different masking models for various kinds of attacks. In [10], Yan Haowen proposed a watermarking technique by shuffling the cover image, extracting the feature points of the data which are grouped as clusters and then the watermark is embedded in the LSBs. This system is proposed mainly to protect copyrights. No intensive experiments were conducted which gives the main drawback of this technique. An enhancement of a watermarking algorithm based on kernel fuzzy clustering and singular value decomposition in the complex wavelet transform domain is proposed in [11]. The host image, also referred to as cover image, is decomposed by complex wavelet transform. Then, the singular value of the low-frequency coefficients is selected as an embedded object. Finally, image low-frequency background and high-frequency texture features are used as fuzzy clustering feature vectors to determine the different embedding strength. The results show that the proposed system performs well against different kinds of attacks. Against image rotation (5^o, 15^o) the Normalized Correlation (NC) is going from 0.93 to 0.98 depending on images. Duc-Hung Le *et al* proposed in [12] a new watermarking extraction based on Content Addressing Memory FPGA. They implemented their system on hardware using FPGA to fast watermarking extraction from 2-dimension (2-D) data. The aim of this research was mainly to minimize the data extraction time without taking into account the possibility of attacks which main corrupt these data. In this paper we are proposing a new approach of image clustering which is called Content Addressing Method (CAM) for color images. Using the defined clusters, watermarks are embedded and extracted. The aim of this paper is to show the robustness of this system against image rotation attacks.

3 Watermarking domains

3.1 Spatial vs. frequency domains

The spatial domain techniques are based on direct modification of the values of the image pixels. The watermark is embedded by modifying these pixels. These techniques are simple and computationally efficient, because they modify the color, luminance or brightness values of a digital image pixels, therefore their application is done very easily, and requires minimal computational power [16]. The techniques are generally used with color images.

The Frequency (transform) domain techniques are based on a transformation of the cover image using a reversible transformation. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). However, DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. The watermark is embedded by the modification of the resulting transformation's coefficients. After which, the inverse transformation produces the watermarked image. This approach distributes irregularly the watermark over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult [16].

The watermark is usually embedded in the middle frequencies of the image, avoiding in one side the most important parts of the image (low frequencies) to not disturb the image visualization and avoiding in the other side the parts presented by high frequencies, which are easily destroyed by a compression or a scaling operation.

Compared to spatial domain techniques, the works done using frequency-domain watermarking techniques demonstrates that these techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms. On the other hand, the frequency based techniques are more complicated and require more computational power than spatial techniques.

Other works combine two or more techniques to further performance improvements. Some use combination between frequency-domain techniques and some use combination between frequency and spatial domain techniques in order to compensate for the drawbacks introduced by each.

Our proposed system (scheme) is a spatial-domain watermarking technique. We demonstrate that using our CAM-based algorithm the proposed system resists better to rotation attacks than frequency-based techniques.

3.2 Watermarking properties

There are several properties that researchers are looking to meet at a certain level among which:

1) Robustness: A digital watermark is called robust (vs. fragile/semi-fragile) if it resists a designated class of transformations.
2) Perceptibility: the hidden watermark should not deteriorate too much the perceived quality of the medium.
3) Capacity: how much information can reliably be hidden in the cover image is very important to users especially when the system gives them the ability to change this amount.
4) Complexity: some applications like in telemedicine require real time embedding and/or detection.

A compromise should be set between these properties as they cannot be all met at a high level in the same time.

4 Proposed System

4.1 Watermark Scheme algorithm

Our watermarking scheme proposed in [13] is shown in Fig. 2. It consists of five steps: 1) the cover image is divided into clusters, 2) the watermark image is imbedded into the cover image using clusters, 3) attack the watermarked image, 4) run clustering method again for result image, and 5) extract watermark from the attacked image using clusters.

1. cover image clustering
2. imbed watermark image into cover image using clusters
3. attack watermarked image
4. attacked watermarked image clustering
5. extract watermark from attacked image

Fig. 2: Watermark Scheme Algorithm

4.2 Image Clustering

The clustering method is shown in Fig. 3. The upper 4 bits for each RGB component are used as arguments for a function to produce a value used as address regrouping all entries sharing the same feature. In this paper, this function is taken as simple as concatenating three bits from each. This yields to an address of 9 bits which gives a maximum of 2^9=512 entries in each cluster.

The clustering function $f(x,y,z)$ should be chosen so that the distribution goes uniform as much as possible.

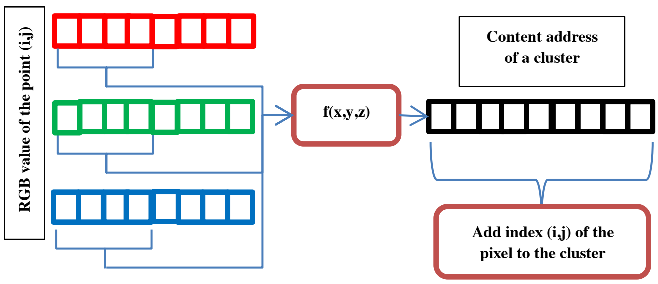


Fig. 3: Clustering Method

The clustering algorithm is going through all cover image pixels and including each pixel indexes in its cluster as shown in Fig. 4.

4.3 Embedding Process

The cover image is scanned using the clusters indexing instead of its own indexing as in Fig. 4. The pixels in each cluster are divided into a number of portions (or sub-cluster), we are using 64, depending on the number of bits that are used to maintain the sequence number of the portion in the cluster (we are using 6 bits). Into each portion are duplicated one to three bits from the watermark image. These settings are parameters that should be chosen according to the number of clusters and the size of the watermark image. The maximum size of the watermark portion embedded in a full cluster is described in Table 1.

The three bits of the watermark image are embedded into 3 of the 4 LSB bits of one of RGB values (say R). The fourth bit is used as parity bit (for error detection). A portion sequence number (counter) is maintained to distinguish between the embedded data and to maintain their sequencing. This counter is written in 3-6 of the LSB bits of the remaining RGB values. A parity bit is also maintained in the fourth bit of each for error detection. The 3 bits extension of the counter is taken from the parity bit protection of the four MSB of RGB values used in [13]. The reason we took out this protection comes from the fact that an image with a certain level of visualization cannot be impacted a lot in its MSB part.

Table 1: Embedded data size per cluster

data_size/counter_size (bits)	Embedded Watermark size per cluster (bits)
3/6	192
2/7	256
1/8	256

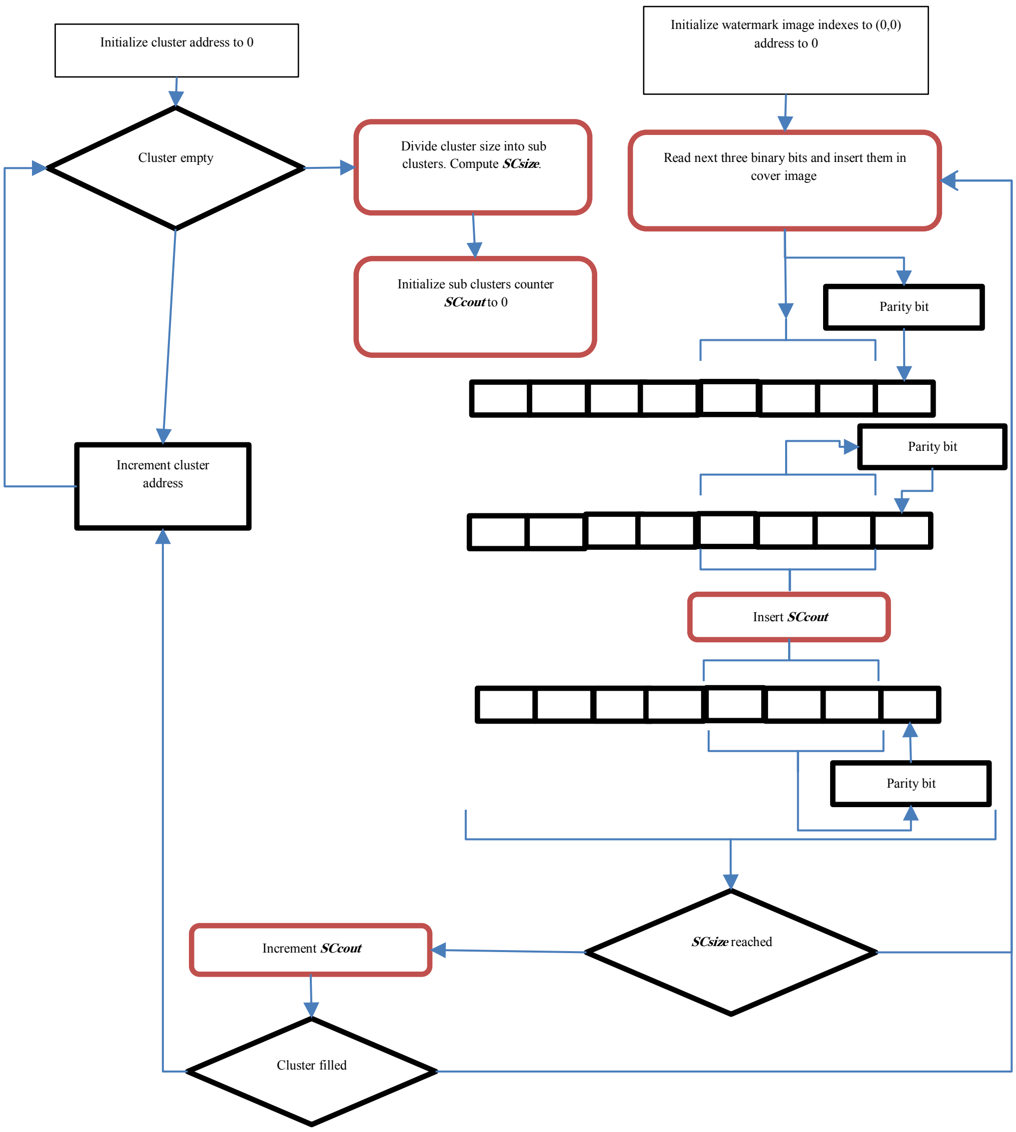


Fig. 4: Embedding Process

4.4 Extracting Process

Fig. 5 is describing the Extracting process algorithm. Before executing the extracting phase, a new clustering process should take place. Again the image should be scanned using the clustering indexing. The watermark should be found in sequence from the first cluster until the last cluster. If the cluster is not empty, all pixels in this cluster are checked, parity bits are verified and a decision table is built as in Fig.5.

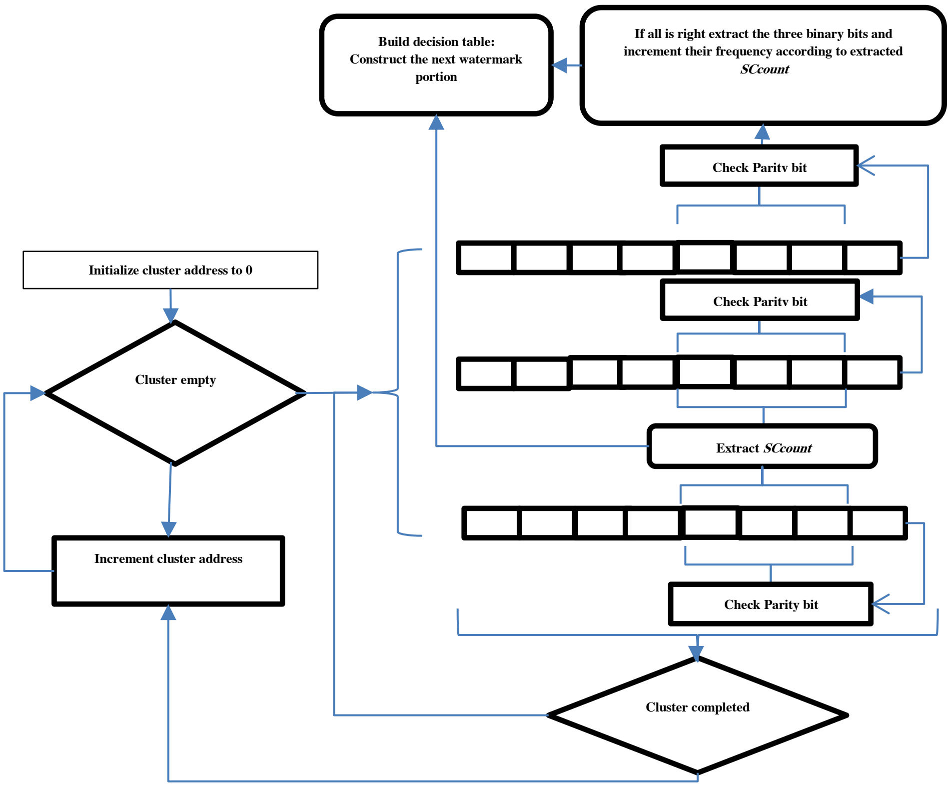


Fig. 5: Extracting process

A decision table is built for the data extracted from each cluster. Fig. 6 presents the decision table. A cluster contains 8x3 bits of watermark data. If a pixel is included in the current cluster and in case all parity bits are checked with no error detection, the counter and the watermark data are extracted and used as indexes to the decision table.

The entry is then incremented giving the number of times the data was found under the same counter without error detection. The column index of the entry with the highest counter gives the data. The order of the 8x3 bits is given by the counter: the first row contains the first three bits etc…

The drawback of this method is caused by the non-detected errors which are represented here by multiple non-zero entries in the same row. The difficulty of the decision is increased when more than one entry with high values close to each other. This problem is reduced when using big clusters sizes.

Increment the entry indexed by the value of extracted 3 bits

row indexed by SCcount (first 8 rows of total of 64)

0	0	3	10	0	0	1	0
0	2	0	0	0	0	20	1
0	1	0	1	15	0	0	0
1	0	0	0	10	2	1	3
2	0	11	11	0	0	0	0
0	17	0	0	0	0	0	0
21	0	0	0	0	0	0	0
6	19	0	1	1	0	1	0

Extracted portion of watermark

0	1	1
1	1	0
1	0	0
1	0	0
0	1	0
0	0	1
0	0	0
0	1	0

Fig. 6: Building Decision Table for watermark extraction

4.5 Content based counter

Content Based Counter (CBC) is used to reduce the impact of using a portion sequence counter in a cluster. The algorithm has two phases as shown in Fig. 7:

```
Phase 1: CBC segmentation
for each cluster:
  for each pixel:
    pc=extractCounter();
    addPixel(portion[pc]);
  endfor
endfor
Phase 2: Uniform distribution
numberOfPortions=min(counterSize, clusterSize/minPortionSize)
portionAvgSize= clusterSize/numberOfPortions
for 1 until numberOfPortions
  dist=1 // 1 bit difference between entries
  while sizeCurrentPortion < portionAvgSize
    for each Entry e having distance dist with currentEntry
      if size(e)> portionAvgSize
        pixNbr=min(portionAvgSize- sizeCurrentPortion,
                   size(e)- portionAvgSize);
        move pixNbr from e to CurrentPortion
      endif
    endfor
    dist = dist+1
  endwhile
endfor
```

Fig. 7: Content Based Counter Algorithm

The first phase is a cluster segmentation in portion based on the value in the counter space. This technique is used mainly to not modify the counter location as much as possible and then get better PSNR. Whereas, the second phase consists of redistribute uniformly the pixels within the portions and build consecutive portions sequence. To minimize the modifications, the latter is done using the minimum possible distance between source and destination. The distance is calculated as:

$$\mathrm{distance}(C_s, C_d) = \sum_{\mathrm{bit0}}^{\mathrm{Csize}} \mathrm{xor}(C_s, C_d) \quad (1)$$

Where C_s and C_d are source and destination counters respectively and C_{size} is the counter size in bits. The complexity of this algorithm is at most *O(MxN)* where *MxN* is the size of the image because it is bounded by visiting all pixels.

5 Experimental Results and Analysis

We used 512×512×3 color images as a host carrier signal, and 64×64 binary image as the watermark signal, as shown in Fig. 8 and Fig. 9. The correlation coefficient (NC) in Equation (2) is used for measuring the quantitative similarity between the extracted and embedded watermarking:

$$\mathrm{NC} = \frac{\sum_x \sum_y i(x,y) w(x,y)}{\sum_x \sum_y i^2(x,y)} \quad (2)$$

Where *i* denotes the embedded original watermark and *w* denotes the extracted watermark.

The difference between watermarked image and original host image is evaluated using the Peak Signal to Noise Ratio (*PSNR*). The *PSNR* formula is giving in the Equation (3):

$$\mathrm{PSNR} = 10\log\left(\frac{\max(i^2(x,y))}{\frac{1}{MxN}\sum_{y=1}^{M}\sum_{x=1}^{N}(i(x,y)-w(x,y))^2}\right) \quad (3)$$

a-Peppers b-Mandrill c-Hollyhocks

Fig. 8: Host carrier signal images

Copyright image

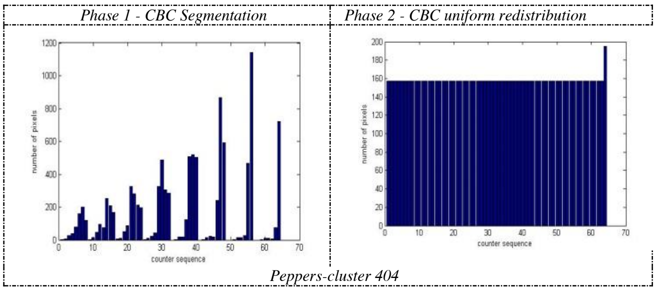
Fig. 9: Watermark signal image

The proposed solution does not affect the normal visualization of the cover image as it is proved by the PSNR presented in Table 2. On the other hand, taking into account the CBC always improves the PSNR.

Table 2: PSNR of cover image

	Peppers	Mandrill	Hollyhocks
Complex Wavelet Transform Domain	45.11	44.83	NA
Our solution without CBC	41.56	44.68	44.00
Our solution with CBC	42.90	45.95	46.18

Fig. 10 gives the result of using CBC technique in different clusters for the different images. Phase 1 in the left column of the figure presents the cluster segmentation based on counter field content and the right column shows the result of the uniform redistribution with minimum cost of pixels.



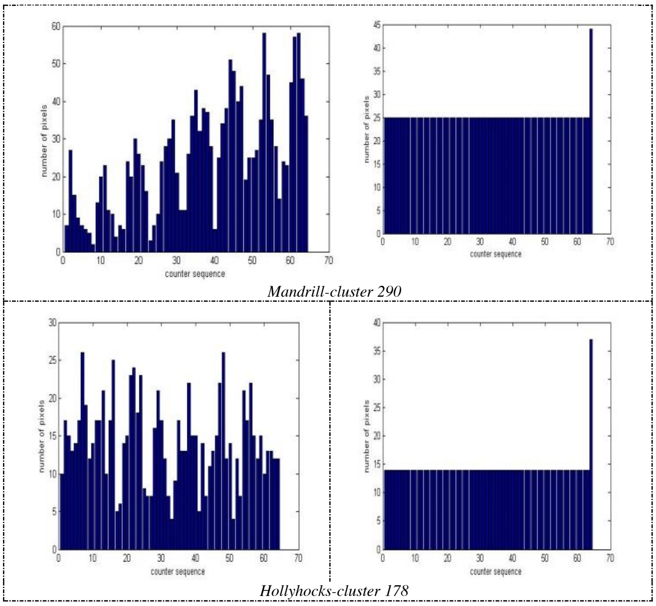


Fig. 10: Content Base Counter Algorithm

Table 3: NBCR of the watermark image(%)

	without CBC	*with CBC*
peppers	3.861	1.492
mandrill	1.962	0.666
Hollyhocks	2.315	0.519

The Number of Bit Change Rate (*NBCR*) given by table 3 confirms the results of *PSNR* improvement given in table 2 by introducing the content based counter. The formula of *NBCR* is given by the Equation 4 where, using a *MxN* image, *Csize* is the counter size and $C_b^{i,j}$ and $C_a^{i,j}$ is the counter value in the pixel *(i,j)* before and after modification respectively.

$$NBCR = \frac{(\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{bit0}^{Csize} xor(C_b^{i,j}, C_a^{i,j}))x100\%}{MxNxCsize} \quad (4)$$

We compared our results with the results provided in [11] under the same environment. Table 4 shows that our system, under rotation attacks for 5° and 15°, the watermark is completely extracted without any distortion (*NC*=1). Fig. 11 shows that under any rotation attack the NC is always equal 1 which proves the robustness of the proposed system against rotation attacks.

Table 4: NC of the watermark image

		Rotation 5°	Rotation 15°
Spatial domain	peppers	0.927	0.885
	mandrill	0.918	0.869
Wavelet domain	peppers	0.945	0.913
	mandrill	0.937	0.896
Complex Wavelet Transform Domain [11]	peppers	0.981	0.946
	mandrill	0.966	0.930
Our solution	peppers	1.000	1.000
	mandrill	1.000	1.000
	Hollyhocks	1.000	1.000

Fig. 12 shows that the new portion allocation technique gives us better results against cropping attacks which was not possible using the First Visited First Allocated *(FVFA*) technique. This is due to the fact that some portions (sub-clusters) completely located on the boundary of the image which, if they are touched by the cropping attack, may impact the embedded watermark. Future work will be concentrated to the way of better distribute the allocation of the sub-clusters.

Looking at the watermarking properties mentioned earlier, our proposed system met them at a certain level as follows:

1) Robustness: we can consider our system more robust against rotation attacks than frequency domain watermarking.

2) Perceptibility: the PSNR of the watermarked image is always above 40 and with the improvement introduced by using CBC technique it reached better than other systems that used the frequency domain.

3) Capacity: as most of the research papers we checked used 64x64 bits watermark size, all our measurements used the same size. On the other hand, by reducing the size of the hidden information per sub-cluster and filing all clusters in the cover image we can reach a size of 256x256.

4) Complexity: the main goal of using spatial domain is to look for better results in terms of robustness remaining in a low complexity level.

6 Conclusion

In this paper we proposed a new watermark system for color images which uses the Content Addressable Method. The cover image is divided into a set of clusters which are built using Content Addressable Method. Each cluster is segmented in its turn into a number of portions. In all pixels of a portion a number of bits (3 bits in our study) of the watermark are duplicated. The robustness of our system comes from the fact that it resists to image rotation attacks. The results show that a rotation of any degree does not have any effect on the embedded watermark which can be extracted without any distortion. Two pixel-to-portion allocation techniques were used. In the first technique, the cluster's pixels are allocated to a portion in a First Visited First Allocated (*FVFA*) way. The counter providing the portion number is added to portions in sequence. In the second technique, a Content Based Counter CBC is used to allocate pixels to the portion and a uniform redistribution is made for each cluster. The redistribution is done in a way to minimize the modifications in counter space. Both techniques show high robustness resisting to rotation attacks. The CBC performs better in terms of Number of Bit Change Rate (*NBCR*) in the counter field. Future work will be concentrated on pushing more experiments on other geometric attacks like cropping as well as JPEG compression and LSBs attacks.

Acknowledgment: The Author gratefully acknowledges financial support for the present work (project ID 2084) from the Deanship of Scientific Research at Qassim University.

References:

[1] L. Xin, L. Xiaoqi , W. Ying, A Semi-Fragile Digital Watermarking Algorithm Based on Integer Wavelet Matrix Norm Quantization for Medical Images, *The 2nd International Conference on Bioinformatics and Biomedical Engineering, 2008. ICBBE 2008.* DOI: 10.1109/ICBBE.2008.189, Publication Year: 2008 , pp. 776–779.

[2] L. Xin, L. Xiaoqi, L. Qiang, Protect Digital Medical Images Based on Matrix Norm Quantization of Digital Watermarking Algorithm, *4th International Conference on Bioinformatics and Biomedical Engineering (iCBBE), 2010*, DOI: 10.1109/ICBBE.2010.5516746, Publication Year: 2010, pp. 1–4.

[3] M.H. Lee, M.F. Horng , B.C. Chang, A DC-based Approach to Robust Watermarking with Hamming-Code, *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007.* IIHMSP 2007, Vol.2, DOI: 10.1109/IIH-MSP.2007.10, Publication Year: 2007, pp. 369 – 372.

[4] S. Laha, J. Chowdhury, A. Khan, S.K. Sarkar, A watermarking scheme based on Singular Value Decomposition and Particle Swarm Optimization, *IEEE 3rd International Advance Computing Conference (IACC), 2013*, DOI: 10.1109/IAdCC.2013.6514344, Publication Year: 2013 , pp. 888–892.

[5] R. Ansari, M.M. Devanalamath, K. Manikantan, S. Ramachandran, Robust Digital image Watermarking Algorithm in DWT-DFT-SVD domain for color images, *International Conference on Communication, Information & Computing Technology (ICCICT), 2012* DOI: 10.1109/ICCICT.2012.6398160, Year: 2012 , pp. 1-6.

[6] H. Zhang, J. Li, C. Dong, Multiple video Zero-Watermarking based on 3D DFT to resist geometric attacks, *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet),* DOI: 10.1109/CECNet.2012.6201983, Year: 2012, pp. 1141–1144.

[7] V.K. Veena, G.J. Lal, S.V. Prabhu, S.S. Kumar, K.P. Soman, A robust watermarking method based on Compressed Sensing and Arnold scrambling, *International Conference on Machine Vision and Image Processing (MVIP), 2012*, DOI: 10.1109/MVIP.2012.6428771, Year: 2012 , pp. 105-108.

[8] A. Mairgiotis, L. Kondi, Y. Yang, Locally optimum detection for additive watermarking in the DCT and DWT domains through non-Gaussian distributions, *18th International Conference on Digital Signal Processing (DSP), 2013*, DOI: 10.1109/ICDSP.2013.6622794, Publication Year: 2013, pp. 1–6.

[9] L. An, X. Gao, X. Li, D. Tao, C. Deng, J. Li, Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking, *IEEE Transactions on Image Processing*, Vol.21 , Issue: 8, DOI: 10.1109/TIP.2012.2191564, Publication Year: 2012, pp. 3598-3611.

[10] Y. Haowen , Watermarking Algorithm for Vector Point Clusters, *7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2011*, DOI: 10.1109/wicom.2011.6040148, Publication Year: 2011, pp. 1–4.

[11] J. Fan, Y. Wu, Watermarking Algorithm Based on Kernel Fuzzy Clustering and Singular Value Decomposition in the Complex Wavelet Transform Domain, *International Conference on Information Technology, Computer Engineering and Management Sciences (ICM), 2011,* Vol.3, DOI: 10.1109/ICM.2011.121, Publication Year: 2011, pp. 42–46.

[12] D.H. Le, T.B.T. Cao, K. Inoue, C.K. Pham, A fast CAM-based Watermarking extraction on FPGA, *International Conference on IC Design & Technology (ICICDT), Italy, 2013* DOI: 10.1109/ICICDT.2013.6563338, Year: 2013, pp. 207-210.

[13] M.T. Ben Othman, New Image Watermarking Scheme based on Image Content Addressing Method, accepted in *13th WSEAS International Conference on Applied Computer and Applied Computational Science ACACOS'14*, Kuala Lumpur, Malaysia, April 23-25, 2014.

[14] J.A. Hussein, Spatial Domain Watermarking Scheme for Colored Images Based on Log-average Luminance, *Journal of Computing*, vol. 2, No. 1, 2010, pp. 100-103.

[15] J. Manoharan, C.Vijila and A.Sathesh, Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks, *International Journal of Security (IJS)*, Vol. 4, No. 3, 2010, pp. 28-37.

[16] D. Asatryan and N. Asatryan, Combined spatial and frequency domain watermarking, *in Proceedings of the 7th International Conference on Computer Science and Information Technologies*, pp. 323-326, 2009.

[17] Doroshin, A. V., Neri, F. (2014) Open research issues on Nonlinear Dynamics, Dynamical Systems and Processes. WSEAS Transactions on Systems, 13, in press.

[18] Ciufudean, C., Neri, F. (2014) Open research issues on Multi-Models for Complex Technological Systems. WSEAS Transactions on Systems, 13, in press.

[19] Neri, F. (2014) Open research issues on Computational Techniques for Financial Applications. WSEAS Transactions on Systems, 13, in press.

[20] Karthikeyan, P., Neri, F. (2014) Open research issues on Deregulated Electricity Market: Investigation and Solution Methodologies. WSEAS Transactions on Systems, 13, in press.

[21] Panoiu, M., Neri, F. (2014) Open research issues on Modeling, Simulation and Optimization in Electrical Systems. WSEAS Transactions on Systems, 13, in press.

[22] Neri, F. (2014) Open research issues on Advanced Control Methods: Theory and Application. WSEAS Transactions on Systems, 13, in press.

[23] Hájek, P., Neri, F. (2013) An introduction to the special issue on computational techniques for trading systems, time series forecasting, stock market modeling, financial assets modeling WSEAS Transactions on Business and Economics, 10 (4), pp. 201-292.

[24] Azzouzi, M., Neri, F. (2013) An introduction to the special issue on advanced control of energy systems (2013) WSEAS Transactions on Power Systems, 8 (3), p. 103.

[25] Bojkovic, Z., Neri, F.(2013) An introduction to the special issue on advances on interactive multimedia systems WSEAS Transactions on Systems, 12 (7), pp. 337-338.

[26] Pekař, L., Neri, F. (2013) An introduction to the special issue on advanced control methods: Theory and application (2013) WSEAS Transactions on Systems, 12 (6), pp. 301-303.

[27] Guarnaccia, C., Neri, F. (2013) An introduction to the special issue on recent methods on physical polluting agents and environment modeling and

simulation WSEAS Transactions on Systems, 12 (2), pp. 53-54.

[28] Neri, F. (2012) An introduction to the special issue on computational techniques for trading systems, time series forecasting, stock market modeling, and financial assets modeling WSEAS Transactions on Systems, 11 (12), pp. 659-660.

[29] Muntean, M., Neri, F. (2012) Foreword to the special issue on collaborative systems WSEAS Transactions on Systems, 11 (11), p. 617.

[30] Pekař, L., Neri, F. (2012) An introduction to the special issue on time delay systems: Modelling, identification, stability, control and applications WSEAS Transactions on Systems, 11 (10), pp. 539-540.

[31] Volos, C., Neri, F. (2012) An introduction to the special issue: Recent advances in defense systems: Applications, methodology, technology WSEAS Transactions on Systems, 11 (9), pp. 477-478.

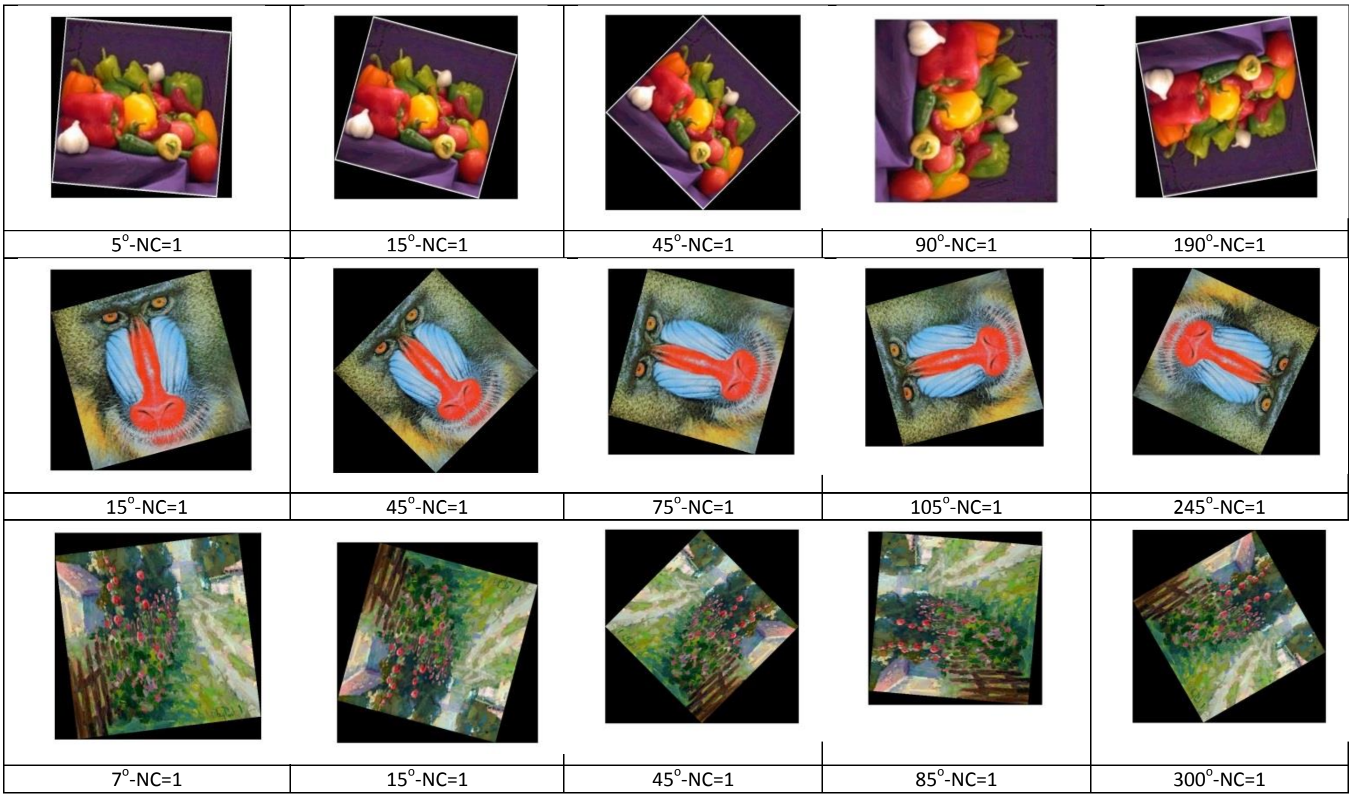
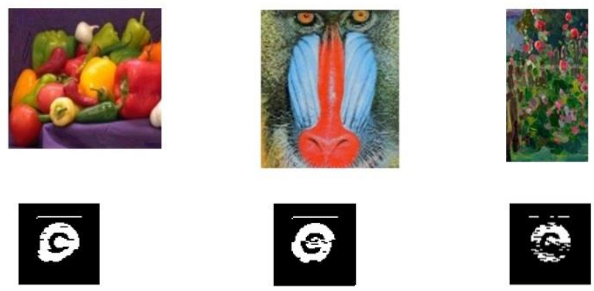


Fig. 11: Different rotation attacks with NC=1



Cropping Peppers to [1,75,440,400] | Cropping Mandrill to [47,45,400,400] | Cropping Hollyhocks to [75,100,190,415]

Fig. 12: Extracted watermark after cropping attacks