

MULTIPLE MESSAGES WATERMARKING IN DIGITAL IMAGE

Garima Anand¹, Ishpreet Virk²

¹ M.Tech Scholar, Computer Science Department, BBSBEC, Fatehgarh Sahib, Punjab (India)

² Assistant Professor, Computer Science Department, BBSBEC, Fatehgarh Sahib, Punjab (India)

ABSTRACT

Image watermarking has become an important tool for intellectual property protection and authentication. In this paper a watermarking technique is suggested that incorporates multiple watermarks in a host image for improved protection and robustness. To protect copyright of images DWT - DCT image watermarking is used. In this paper CDMA approach of embedding watermark is taken so that maximum number of watermarks can be embedded in original image to increase its authenticity. After embedding the watermarks the PSNR values are calculated at each watermark embedding and a table is constructed showing PSNR at each level. At the receiver end retrieval of watermark is done by correlation of original image. Furthermore, to test the robustness of the technique, the watermarked image was exposed to some types of attacks, namely compression, low pass filtering, salt and pepper noise and luminance change.

Keywords – CDMA, DWT, DCT, Viterbi, Image Watermarking, Wavelets

I. INTRODUCTION

Digital watermarking is similar to watermarking physical objects except that the digital watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format. The digital watermarking system essentially consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks. Watermark can be a number, text or image. Secret/public key is used to enforce security of watermarked content. For secure transport of watermarked data encryption/decryption is used. Watermark can be recovered by an authorized agency having secure key, watermark and / or original data.

II. METHODOLOGY

By using proposed approach we embed invisible watermark into image called invisible watermarking. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such. The watermark may be intended for widespread use and thus, is made easy to retrieve or it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In visible watermarking, the objective is to attach watermark or other descriptive information to the signal in a way that is difficult to remove. In the proposed algorithm, first convert the message into sequence of 1 and 0. After that, generate the PN sequence that will be kept same for complete embedding process. After that, perform the DWT on the host image to decomposing image into non-overlapping sets and then choose the block size and perform the DCT on block and embed with PN sequence after performing for each block, perform IDWT on updated values. Same process will be used for embedding more images on the host image and while retrieving the image, DWT-DCT joint algorithm is used. DCT is performed on block on the basis of mid band and generate the sequence and correlate it with PN sequence. Repeat the above step for each blocks and then reshape the message vector and that message is very much similar to original image.

III. PROPOSED ALGORITHM

3.1 Watermark Embedding

Step 1: Take the message and reformulate the message into sequence of 1 and 0.

Step 2: Convolutionally encode the message and this encoded message is further used for processing.

Step 3: Take the key and generate a PN sequence by that key. This PN sequence is kept same during all embedding process.

Step 4: Generate two highly uncorrelated PN sequence pn_sequence_1 and pn_sequence_0.

Step 5: Perform DWT on the host image to decompose it into four non-overlapping multi resolution coefficient sets: cA1, cH1, cV1 and cD1.

Step 6: Choose block size and a mid band coefficients matrix for DCT. In our paper block size of 8 is chosen and a mid band

matrix of 8*8 is chosen from literature review.

Step 7: Now perform DCT on cH1 and embed both PN sequence with a gain factor 'k' depending on the bit value of message.

The algorithm for embedding PN sequence is shown as

$$\mathbf{X} = \mathbf{x} + \mathbf{k} * \mathbf{PN0} \text{ if } \mathbf{b} = \mathbf{0}$$

$$\mathbf{X} = \mathbf{x} + \mathbf{k} * \mathbf{PN1} \text{ if } \mathbf{b} = \mathbf{1}$$

Where,

x = is the cover image

b = is the watermarked bit

X = is the embedded image

Step 8: Now perform IDCT on cH1.

Step 9: Repeat step 6 and 7 for cV1.

Step 10: Perform IDWT on updated values of cA1, cH1, cV1, cD1 and name this image as watermarked image.

Step 11: PSNR and Normalized cross correlation is found out to determine robustness and image quality of watermarked image.

Step 12: Now follow steps from 1 to 10 for embedding next watermark using separate key for PN sequence. The size of watermark is determined by hit and trial method and that comes less than the previous watermark size.

Step 13: Number of watermarks embedded depends upon retrieval process because watermark should be retrieved properly that is without any distortion.

3.2 Watermark Retrieval

The joint DWT-DCT algorithm is a blind watermarking algorithm, and thus the original host image is not required to extract the watermark.

Step 1: Steps from 1 to 5 of embedding process are same using same key for PN sequence generation.

Step 2: Now perform DCT on cH1 and generate a sequence at condition where mid band matrix element is 1.

Correlate that

sequence to pn_sequenc_0 and to pn_sequence_1.

Step 3: Repeat the step 2 with cV1.

Step 4: Take the mean of correlation value for pn_sequence_1 of cH1 and cV1 and correlation value for pn_sequence_0 of cH1 and cV1.

Step 5: If correlation value for 0 is greater than the correlation value of 1, put the message vector element equal to 0 otherwise 1

correlation_0 > correlation_1

Message vector = 0

Otherwise

Message vector = 1

Step 5: Apply viterbi decoder on message vector to decode message vector into original.

Step 6: Reshape the message vector and that will be similar to message embedded.

Step 7: Same steps are repeated for next watermark message retrieval.

IV. RESULTS

In this paper, Matlab's image processing toolbox is used to show the result. To make our result more precisely, image has been categorized into three different categories depending on the intensity of image. The categories are: low key image, high key image and medium key image.

4.1 Watermark Embedding

In embedding process three messages have been embedded in the cover image. It has been observed that the message size goes on decreasing with increase in the number of messages embedded in the cover image. Below given table shows our three messages embedded in the cover image along with their size.

1 st Message	Copyright	20*50
2 nd Message	CS	9*12
3 rd Message	W	27*22

Table 1: Three Messages To Be Embedded

Below given figures show the result after embedding three messages in the low key image first and after Gaussian noise added into them.



Fig 2: Cover Image



Figure 3: Watermarked Image for 1st Message



Fig 4: Gaussian Noise Embedded



Fig 5: Watermarked Image for 2nd message



Fig 6: Gaussian Noise Embedded



Fig 7: Watermarked Image for 3rd message



Fig 8: Gaussian Noise Embedded

4.2 Watermark Retrieval

Table 2 shows the retrieved messages. It is showing different messages retrieved for different intensity images. All three messages embedded in an image are retrieved for every type of image for same gain $k = 8$.

		Original Watermark	Recovered Watermark
Low Key Image	1 st Message	Copyright	Copyright
	2 nd Message	CS	CS
	3 rd Message	W	W
High Key Image	1 st Message	Copyright	Copyright
	2 nd Message	CS	CS
	3 rd Message	W	W
Medium Key Image	1 st Message	Copyright	Copyright
	2 nd Message	CS	CS
	3 rd Message	W	W

Table 2: Retrieved Watermark Messages

V. ANALYSIS

The clarity of retrieved message depends upon the value of gain factor. This value differs from image to image. For example as clear from table 1, for the same value of 'k', messages for high key image and medium key image are not retrieved properly. Below given tables are showing different PSNR values, Image fidelity and Normalized Cross Correlation values for different values of 'k'.





S No.	k	PSNR	NCC	Retrieved Message
1	8	50.4760	1.0000	
2	10	45.6435	1.0000	
3	16	36.3215	1.0000	
4	28	27.0312	1.0005	

Table 3: Retrieved Messages for Different Values of K for 1st Message in Low Key Image




S No.	k	PSNR	NCC	Retrieved Message
1	8	51.0983	0.9998	
2	18	34.3483	0.9982	
3	28	26.7608	0.9942	

Table 4: Retrieved Messages for different values of k for 1st message in High Key Image


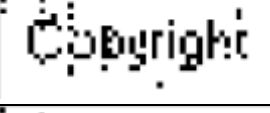


S No.	k	PSNR	NCC	Retrieved Message
1	8	53.5525	1.0000	
2	10	48.6215	1.0000	
3	12	44.7038	1.0000	
4	18	36.7019	0.9999	

Table 5: Retrieved Messages for different values of k for 1st message in Medium Key Image




S No.	k	PSNR	NCC	Retrieved Message
1	8	50.8496	1.0000	
2	10	48.9073	1.0000	
3	28	40.3796	1.0001	

Table 6: Retrieved Messages for different values of k for 2nd message in Low Key Image






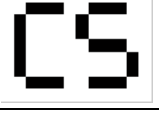
S No.	k	PSNR	NCC	Retrieved Message
1	8	51.3974	0.9998	
2	10	49.4345	0.9998	
3	12	47.8318	0.9998	
4	14	46.6110	0.9997	
5	16	45.3831	0.9997	
6	28	40.5847	0.9994	

Table 7: Retrieved Messages for different values of k for 2nd message in High Key Image




S No.	k	PSNR	NCC	Retrieved Message
1	8	50.5714	1.0000	
2	10	48.5917	1.0000	
3	12	46.9742	1.0000	

Table 8: Retrieved Messages for different values of k for 2nd message in Medium Key Image

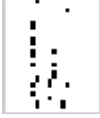




S No.	k	PSNR	NCC	Retrieved Message
1	8	51.0085	1.0001	
2	10	46.1348	1.0001	
3	18	34.6542	1.0003	
4	24	29.8072	1.0007	
5	28	27.3050	1.0011	

Table 9: Retrieved Messages for different values of k for 3rd message in Low Key Image

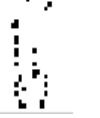
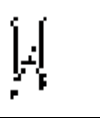

S No.	k	PSNR	NCC	Retrieved Message
1	8	51.4022	0.9944	
2	16	36.8303	0.9976	
3	28	27.0165	0.9998	

Table 10: Retrieved Messages for different values of k for 3rd message in High Key Image




S No.	k	PSNR	NCC	Retrieved Message
1	8	50.5443	1.0000	
2	16	35.8808	1.0000	
3	28	25.8813	0.9988	

Table 11: Retrieved Messages for different values of k for 3rd message in Medium Key Image

Above given tables show that as the number of messages to be embedded is increased, the PSNR also increases but normalized cross correlation has to be compromised a bit. Perfect retrieval of message is from high key image for high PSNR values. High PSNR value means high robustness of watermarked image. PSNR values are higher for medium key image than others for all values of k. that's why medium key image is more robust than others but appropriate retrieval of message from medium key image is for PSNR=36.7019 i.e. less robustness of watermarked image. In the retrieval of second message, PSNR is high for high key image. Below showing graphs are showing the plot of PSNR and gain values for all three messages embedded in low key image. The PSNR value is highest for second message in low key image followed by third message. Although as retrieved messages table speaks, third message is not retrieved properly at higher PSNR values.

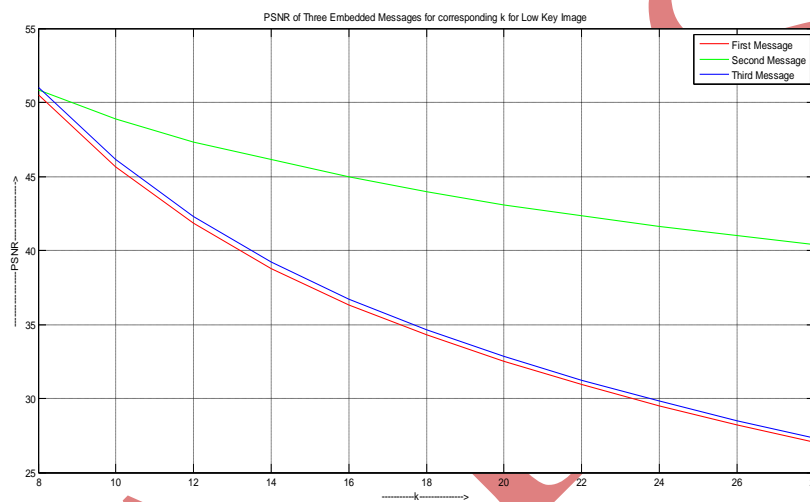


Figure 9: PSNR values for different gain factors in low key image for three embedded messages

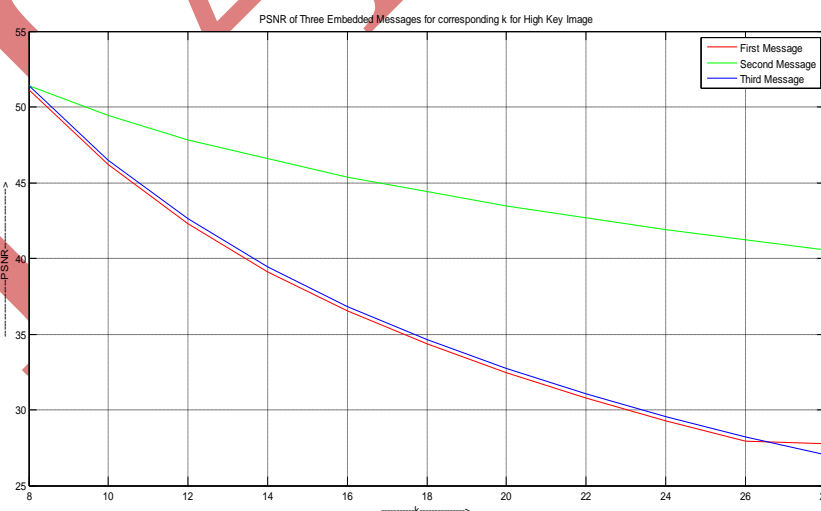


Figure 10: PSNR values for different gain factors in high key image for three embedded messages

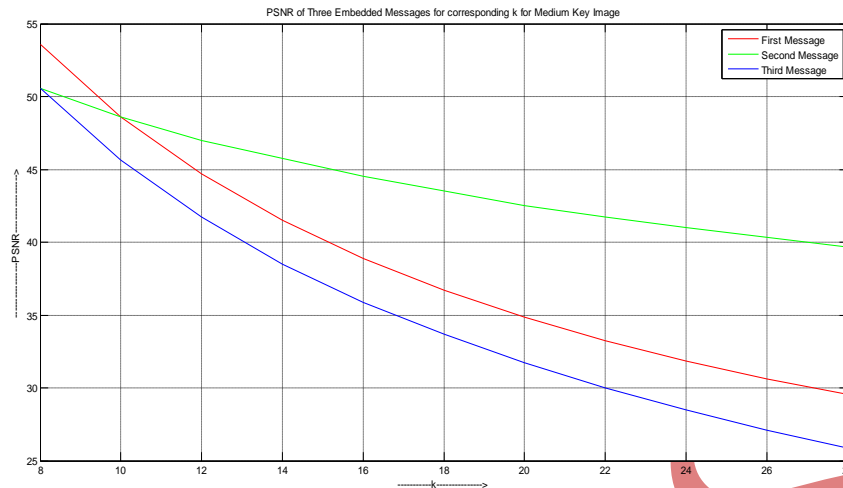


Figure 11: PSNR values for different gain factors in medium key image for three embedded messages

VI. CONCLUSION

The effectiveness of the whole scheme is proven through simulation results like:

- 1) PSNR quality assessment objectives are achieved
- 2) Watermarked image have very good visual quality
- 3) No auxiliary data is required for quality estimation (only embedded watermarks and test images are needed).

In this work, a still image watermarking scheme with high robustness in the frequency domain is applied. The proposed scheme tests only image rather than audio or video. This algorithm can be used for data hiding in many applications such as authentication and copyright protection.

Proposed watermarking system has following advantages:

1. The proposed invisible watermarking system is secure as the data is stored in different segments of the images randomly. There is no static area to store data in image. In this work area will be selected dynamically by the proposed system itself.
2. The proposed system is efficient as more than one message is hidden in the image that makes it more robust as proved with increase in PSNR values. The proposed system is easy to understand with basic knowledge of the matrix.
3. Typically proposed technique is computationally pricey, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images Even if the algorithm is know it is not easy to retrieve the data.

Image Quality	Very Good	Good	Acceptable	Poor
PSNR(dB)	≥ 40	35-40	30-35	< 30

Table 12: PSNR level

From the table 12 it is clear that my scheme falls in the category of ‘Very Good’ in the case of 1st, 2nd and 3rd embedded message my scheme comes in the category of ‘Very Good’. Thus even many messages are embedded into an image my scheme is proven very good on PSNR basis.

VII. FUTURE WORK

Watermarking is an emerging research area for copyright protection and authentication of the multimedia. Most of the research is going on in this field; the reason might be that there are so many images available at internet without any cost, which needs to be protected. The watermarking technique that is given in this dissertation can be further extended by implementing Cat Swarm optimization method after the DWT. In future, work may be extended on different media like video, audio etc by using this approach. Right now the proposed approach is working only with the images. In this dissertation water marks are embedded with the help of DWT- DCT- Viterbi. So, further work can be done to find some other watermark embedding scheme to increase the security of Watermarked data.

REFERENCES

- [1] Chiou-Ting Hsu and Ja-Ling Wu, “Hidden Digital Watermarks in Images” , *IEEE Transactions On Image Processing*, Vol. 8, No. 1, PP. 58-68 1999.
- [2] A.K. Vanwasi, “Digital Watermarking-Steering the Future of Security”, *Network Magazine, Indian Enterprise Group, Mumbai Edition*, 2001.
- [3] Athanasios Nikolaidis and Ioannis Pitas, “Region-Based Image Watermarking”, *IEEE Transaction On Image Processing*, Vol.10, No.11, PP. 1726 – 1740, 2001.
- [4] Christian S. Collberg, Member and Clark Thomborson, “Watermarking, Tamper- Proofing, and Obfuscation Tools for Software Protection”, *IEEE Transactions on Software Engineering*, Vol. 28, No. 8, PP. 735-746, 2002.
- [5] FrankY. Shih, Scott Y.T. Wu, “Combinational image watermarking in the spatial and frequency domains” *Science Direct*, Vol. 36, No. 4, PP. 969-975, 2002.
- [6] Mauro Barni, Franco Bartolini, Alessia De Rosa, and Alessandro Piva, “Optimum Decoding and Detection of Multiplicative Watermarks”, *IEEE Transaction On Signal Processing*, Vol. 51, No. 4, PP. 1118-1123, 2003.
- [7] Ping Dong, Jovan G. Brankov, Nikolas P. Galatsanos, Yongyi Yang, Franck Davoine, “Digital Watermarking Robust to Geometric Distortions” *IEEE Transactions on Image Processing*, Vol. 14, No. 12, PP. 2140 – 2150, 2005.
- [8] Khaled Mahmoud, Sekharjit Datta, and James Flint, “Frequency Domain Watermarking: An Overview”, *The International Arab Journal of Information Technology*, Vol. 2, No. 1, PP.33-47, 2005.
- [9] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, “A Dual Digital-Image Watermarking Technique”, *World Academy of Science, Engineering and Technology 5*, 2005.
- [10] Kamran Hameed, Adeel Mumtaz, and S.A.M. Gilani, “Digital Image Watermarking in the Wavelet Transform Domain”, *World Academy of Science, Engineering and Technology*, Vol.13, PP. 86-89, 2006.

- [11] Nasrollah Moghaddam Charkari, Mohammad Ali Zare Chahooki, “A Robust High Capacity Watermarking Based on DCT and Spread Spectrum”, *IEEE International Symposium on Signal Processing and Information Technology*, 2007.
- [12] Saraju P. Mohanty, Bharat K. Bhargava, “Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks”, *ACM Journal*, Vol. V, No. N, PP. 1–24. 2008.
- [13] Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, “A New Robust Digital Image Watermarking Technique Based On Joint DWT DCT Transformation”, *Third 2008 International Conference on Convergence and Hybrid Information Technology*.
- [14] P. Viswanathan, Dr. P. Venkata Krishna, “Text fusion watermarking in Medical image with Semi-reversible for Secure transfer and Authentication”, *IEEE International Conference on Advances in Recent Technologies in Communication and Computing*, PP. 585 – 589, 2009.
- [15] Sadasivam Subbarayan, S.Karthick Ramanathan, “Effective Watermarking of Digital Audio and Image using Matlab Technique”, *Second International Conference on Machine Vision*, 2009.
- [16] Liu Ping Feng, Liang Bin Zheng, Peng Cao, “A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection”, *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, 2010.
- [17] Satyanarayana Murty. P, Dr. P. Rajesh Kumar, “A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DCT-SVD Technique”, *IJCSNS International Journal of Computer Science and Network Security*, VOL.10 No.10, 2010.
- [18] Hossein Rahmani, Reza Mortezaei, and Mohsen Ebrahimi Moghaddam, “A New Robust Watermarking Scheme to Increase Image Security”, *EURASIP Journal on Advances in Signal Processing*, Vol. 2010, No. 428183, PP. 30, 2010.
- [19] Dhruv Arya, “A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques”, *International Journal of Scientific & Engineering Research*, Volume 1, Issue 2, 2010.
- [20] Afrin Zahra Husaini & M. Nizamuddin, “Challenges and Approach for a Robust Image Watermarking Algorithm”, *International Journal of Electronics Engineering*, Vol. 2, PP. 229-233, 2010.