Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 2, pp: (1-4), Month: May - August 2015, Available at: www.noveltyjournals.com

Enhanced Digital Watermarking Technique for Image Cryptography

[1]Anjali Sharma, [2]Pradeep Kumar Singh

[1]M.TECH Student, CSE Department, Amity University, Noida, India
[2]Assistant Professor, CSE Department, Amity University, Noida, India

Abstract: **In this paper a robust image watermarking technique has been presented i.e. Discrete Cosine Transform. Watermarked data is encrypted for the cryptography purpose. The main stratagem for the approach is to enhance capacity and security feature. Capacity is increased by the nesting technique as per which we will embed watermark into watermark. The frequency domain is used in this research as the spatial domain is less robust than this. Though the spatial domain is less time consuming but robustness is the most important factor to be considered for cryptography.**

Keywords: **DCT, Image Watermarking, PSNR, Cryptography**

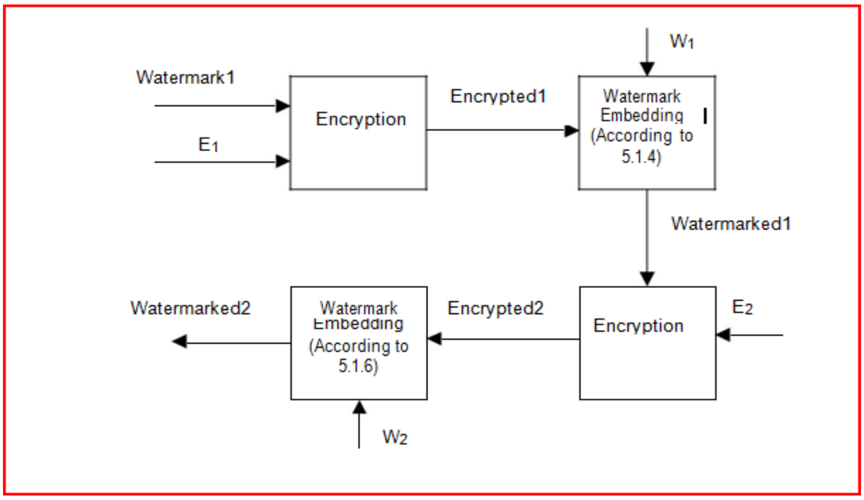
I. INTRODUCTION

In layman terms if we describe watermarking then it is more like inserting your information in a physical object just like when we see a 100 rupees note, a sequence of numbers are inserted into it to detect from a fake currency. And we use the same concept for digital watermarking then we have all the signals available as digital content. In this a signal with low energy is taken. This signal is then embedded into another signal. The signal with low energy is considered as a watermark. This signal may contain a sequence of bits, digital signatures, your credit card number or any information critical data that cannot be transferred in plain text. This is then embedded into original signal. We call this signal as cover signal. This actually covers the watermark. We can consider a cover signal as a stand-alone picture/image, audio clip, video clip or any digital document in digital format.

The system for digital watermarking consists of mainly three components; first one is embedder or watermark embedder. In this embedder we embed low energy signal which we call watermark into main signal which we called cover signal. For every secure contents there has to be a secure or private key. This key identifies the uniqueness of watermark signal. The second component is communication path or we can say communication channel from which watermark signal has to be travelled. On which unauthorized person can attack and it may contain noisy data that may try to modify digital content of the watermark. Then we have third component which is called as watermark detector. This block helps to take out the watermark signal or to identify the watermark signal from the embedder. The key used in watermarking has to follow one to one correspondence which means that every single watermark would have lots of separate unique key to identify its identity. These private keys are to be known by only legal parties so that to provide surety that it can only be identified by the authorized users. Moving forward, we have communication channel which can easily be susceptible to noise hence we should brought a watermarking technique that should be resistant to these noisy signals.

II. IMPLEMENTATION

The block diagram for the encrypted watermark image transmission is given below.



Watermark1 is taken. It is encrypted by using XOR operation. Encryption key E1 is used. We will get Encrypted E1 as output. Encrypted E1 is now embedded in the watermark2. Key W1 is used and the image received in output is watermarked1. Now watermarked watermark will be encrypted using XOR operation and key E2 is used. The output of this will be Encrypted 2. Now the output received in step 3 will now be embedded in grey scale cover image. Key W2 is used. And the output received from this step will be final watermarked image.

We have considered a single image. We measure the quality of watermarked images in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case PSNR should be infinite and MSE should be zero. But it is not possible for watermarked image. So, large PSNR and small MSE is desirable. To see that if the recovered watermark is identical to the one that is embedded we calculate only MSE. In this case it should be zero.

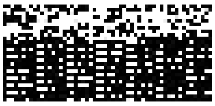
III. EXPERIMENTAL RESULTS AND ALGORITHM

Fig.2 Input Image

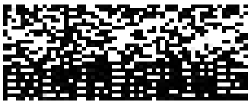
The ‘LENA’ image is used as the input image in which watermark image is embedded. First we see the effect of embedding nested watermark in each image.

Fig.3 Watermark Image

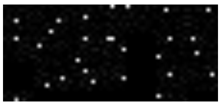
The image given in the figure above is used as the watermark in the input image of LENA. The watermarked image is then encrypted and the final output image is obtained with the invisible watermark.



Original Watermark



Watermarked Watermark



Difference

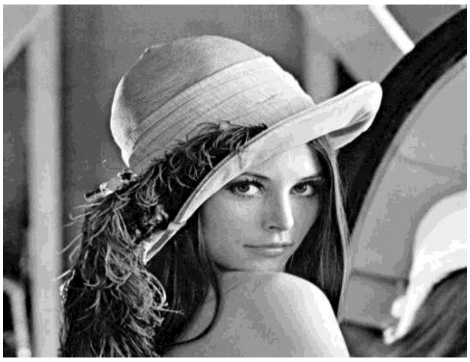


Fig.4 Output Image with Invisible Watermark

```
function y=psnr(processed,original)
processed=im2double(processed);
original=im2double(original);
[m n]=size(original);
%mserror
error=processed - original;
se=error.*error;
sumse=sum(sum(se));
mse=sumse/(m*n);
%mserror
ma=max(max(processed));
y=10*log10(ma*ma/mse);
```

Image	Wm1	Wm2	PSNR1	MSE1	PSNR2	MSE2
Lena (512 × 512)	h.bmp (12 × 12)	Lenatext.bmp (27 × 56)	17.3239 dB	0.0185	37.1587dB	11.736

Table.1. PSNR and MSE Calculation

IV. FUTURE SCOPE AND CONCLUSION

Information security is an uprising field. Watermarking is contribution to it. Number od researches and studies are coming into practice day by day. This is further getting used in copyright protection and to provide security to the data which is available online. The data is more in the form of multimedia contents like audio, video, text, etc. The DCT technique has provided the better results in the frequency domain in terms of robustness which can further be enhanced with the replacement of DCT with Discrete Wavelet Transform i.e. DWT. By the use of DWT we are able to insert more number of bits to the watermark as compare to the methodology which is without nesting watermarking.

REFERENCES

[1] Aboofazeli, M., Thomas, G., Moussavi, Z., ”A wavelet transform based digital image watermarking scheme”, in IEEE Canadian Conference on Electrical and Computer Engineering, Vol. 2, pp. 823 – 826, May 2004.

[2] Alper Koz, “Digital Watermarking Based on Human Visual System”, The Graduate School of Natural and Applied Sciences, The Middle East Technical University, pp 2 – 8, Sep 2002.

[3] Amara Graps, “An Introduction to Wavelets”, in IEEE Computer Science and Engineering, vol. 2, num. 2, pp. 50-59, 1995.

[4] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, “A SURVEY ONWATERMARKING APPLICATION SCENARIOS AND RELATEDATTACKS”, IEEE international Conference on Image Processing, Vol. 3, pp. 991–993,

[5] Deepthi Anand, U.C. Niranjan, “Watermarking Medical Images With Patient Information”, in Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 20, No 2, pp. 703 – 706, 1998.

[6] Dr. Martin Kutter and Dr. Frederic Jordan, “Digital Watermarking Technology”, in AlpVision, Switzerland, pp 1– 4.

[7] Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan, “Hiding Watermark in Watermark”, in IEEE International Symposium in Circuits and Systems (ISCAS), Vol. 4, pp. 4018 – 4021, May 2005.

[8] Frank Hartung, Martin Kutter, “Multimedia Watermarking Techniques”, Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103, July 1999.

[9] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, “ A Secure Data Hiding Scheme for Two-Color Images”, in Fifth IEEE Symposium on Computers and Communications, pp. 750 – 755, July 2000.

[10] J.J.K.O. Ruanaidh, W.J.Dowling, F.M. Boland, “Watermarking Digital Images for Copyright Protection”, in IEE ProcVis. Image Signal Process., Vol. 143, No. 4, pp 250 - 254. August 1996.

[11] Kaewkamnerd, N., Rao, K.R., "Multiresolution based image adaptive watermarking scheme", in EUSIPCO, Tampere, Finland, Sept. 2000.