

Image and Video based double watermark extraction spread spectrum watermarking in low variance region

Mriganka Gogoi

Electronics and Communication
Assam Don Bosco University
Guwahati,India

H.M.Khalid Raihan Bhuyan

Electronics and Communication
Assam Don Bosco University
Guwahati,India

Koushik Mahanta

Electronics and Communication
Assam Don Bosco University
Guwahati,India

Dibya Jyoti Das

Electronics and Communication
Assam Don Bosco University
Guwahati,India

Ankita Dutta

Electronics and Communication
Assam Don Bosco University
Guwahati,India

Abstract— Digital watermarking plays a very important role in copyright protection. It is one of the techniques which are used for safeguarding the origins of the image, audio and video by protecting it against Piracy. This paper proposes a low variance based spread spectrum watermarking for image and video in which the watermark is obtained twice in the receiver. The watermark to be added is a binary image of comparatively smaller size than the Cover Image. Cover Image is divided into number of 8x8 blocks and transform into frequency domain using Discrete Cosine Transform. A gold sequence is added as well as subtracted in each block for each watermark bit. In most cases, researchers has generally used algorithms for extracting single watermark and also it is seen that finding the location of the distorted bit of the watermark due to some attacks is one of the most challenging task. However, in this paper the same watermark is embedded as well as extracted twice with gold code without much distortion of the image and comparing these two watermarks will help in finding the distorted bit. Another feature is that as this algorithm is based on embedding of watermark in low variance region, therefore proper extraction of the watermark is obtained at a lesser modulating factor. The proposed algorithm is very much useful in applications like real-time broad casting, image and video authentication and secure camera system. The experimental results show that the watermarking technique is robust against various attacks.

Keywords—Watermark;Gold Code; Variance; Correlation.

I. INTRODUCTION

Digital watermarking plays a very important role in multimedia transmission. Consequently, digital watermark technique needs to be incorporated in digital rights to address different aspects of the content supervision. Due to the availability of digital equipments and rapid development of internet, access to digital information has become very easier. As a result protection of copyright and intellectual property of

the media has become very much essential. Digital watermarking came as an efficient solution of the above mention. The watermarking embeds information into the host data in some invisible as well visible way that is supposed to identify the owner .Watermarking schemes can be classified into various ways: There are basically two types of watermarking scheme, spatial domain and frequency domain according to working field. Watermarking in transform domain provides more robustness to the watermarking process. In transform domain, the effect of noise and distortion of original Image during the watermarking process is less. The frequency domain schemes are generally considered more robust than the spatial domain schemes and are based on DCT (discrete cosine transform) and DWT (discrete wavelet transform), Fast Fourier Transform (FFT) in general. In most of transform domain watermarking techniques in which watermark is embedded once and the same is extracted in the receiver. However, if the watermarked image or video undergoes any attacks in the channel then a distorted watermark is obtained in the receiver. But, finding the error of a particular bit in the watermark is quite challenging when the original watermark is not present in the receiver. In this proposed method a single watermark is embedded twice with less distortion in the low variance region of the image. Also, the same watermark is obtained twice, comparing both the watermarks gives the error occurred.

II. RELATED WORK

Previously, some researchers have proposed various papers and implemented different techniques for the watermark algorithm. Ingemar J. Cox et al[1] proposed an algorithm to insert a watermark into the spectral components of the data using techniques analogous to spread spectrum communications, hiding a narrow band signal in a wideband channel that is the data. Mercy George et al[2] proposed the

direct sequence spread spectrum technique of watermarking for video and images which can be used for both special and spectral domain watermarking. T. Kohda et al [3] proposed a color image communication system through code division multiple access (CDMA) channels with spreading sequences of variable-period to transmit YIQ signals. In this paper, they proposed a digital watermarking system where YIQ signal channels and embedded watermark image channel are separately used. R. Bangaleea et al [4] proposed a spatial domain-watermarking scheme for data hiding and copyright protection of still images using the attack characterisation approach. Here they have added two watermarks and used two keys for the watermarking system. The use of the key introduce uncertainty about the location of the watermark bits in spatial domain. Fan Zhang et al[5] proposed Digital Image Watermarking algorithm Based on CDMA Spread Spectrum where orthogonal gold code is used to spread spectrum of the copyright messages. The copyright messages can be extracted without the original image as it is a blind watermarking algorithm. Bo Chen et al [6] proposed a new robust-fragile double image watermarking algorithm. They have used the improved pixel-wise masking model and pseudo-random sequence to embed robust watermark and fragile watermark into the insensitive (robust) part and sensitive part of the wavelet coefficients of the host image. This makes the two watermarks non-interfering and increases the watermarking capacity of the host image without reducing watermark robustness and also the PSNR value is found to be high compared to the single watermarking scheme while considering the same robustness. Xiu-mei Wen et al[7] proposed a digital image watermarking algorithm based on Fourier domain. The fourier transform can embed watermark not only in the amplitude of transform domain but also in the phase degree of transform domain if it is satisfied with the real numbers inverse transform. In this paper, the algorithm embeds the watermark in the amplitude of transform domain.

HO ATS et al[8] has proposed a robust digital image in image watermarking using Fast Hadamard Transform and he pointed out some of the advantages in terms of shorter processing time. Kutter et al[9] embedded the watermark by modifying a selected set of pixels in the blue channel because human eyes are less sensitive to changes in this color channel. The blue channel, however, is the frailest to JPEG compression among the three color channels, so the hidden watermark information is easy to be lost.

III. WATERMARKING ALGORITHM

The watermark algorithm is viewed as a sequence of stages. The block diagram for transmitter and receiver is shown in the transmitter and in the receiver part.

A. Transmitter part

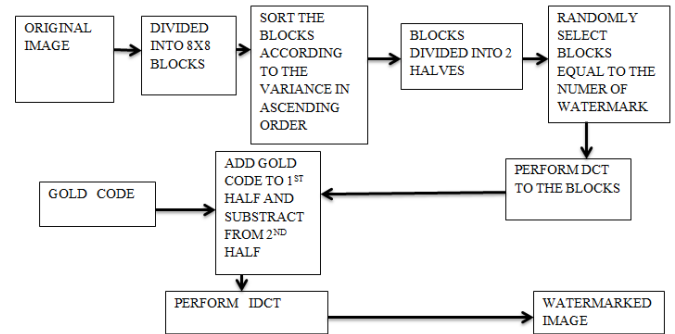


Fig. 1 Watermark embedding block

In the transmitter part, the image is taken from pc and the image is divided into (8x8) blocks. Each block will contain 64 pixel values. The blocks are sorted according to the variance in ascending order. The low variance blocks are then taken because they can create less distortion in the image and so the watermark can easily be extracted by using the algorithm known to sender and the receiver. The equation of variance is given by—

$$\text{Var}(x) = \frac{\sum(x_i - \bar{x})^2}{N} = \frac{\sum x_i^2}{N} \quad (1)$$

Where ‘x’ is a 1D matrix, ‘x̄’ is the mean and ‘N’ is the length of the matrix.

After sorting the blocks according to the variance, the blocks are divided into two halves and half of them are considered having low variance and from those blocks some blocks are randomly selected and with them orthogonal gold codes are added whose number of bits is equal to the randomly selected blocks. Now DCT is performed to the selected blocks. Again the randomly selected blocks are divided into two halves by considering each having 31 AC co-efficients by ignoring the DC co-efficient and the last AC co-efficient. Now by performing XOR operation between two p-n sequences we get a gold code which is added to one half and subtracted from the other half. Now inverse discrete cosine transform of the blocks gives the watermarked image. The equation for watermarking is-

CASE 1-

$$X_w = X_i + m_k g_m \text{ if watermark bit is '1'}. \quad (2)$$

$$X_w = X_i - m_k g_m \text{ if watermark bit is '0'}.$$

CASE 2-

$$X_w = X_i - m_k g_m \text{ if watermark bit is '1'}. \quad (3)$$

$$X_w = X_i + m_k g_m \text{ if watermark bit is '0'}.$$

Where X_w is watermarked image, X_i is the original image, m_k is the modulation factor and g_m is the orthogonal gold code.

B. Receiver Part

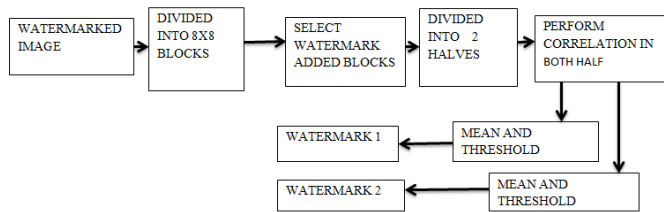


Fig. 2 Watermark extraction block.

In the receiver section, from the watermarked image, blocks in which watermark is added are considered and DCT is performed. Like in the transmitter each block is again divided into two halves eliminating the DC component and last AC co-efficient. Now correlation is obtained between each half and the corresponding gold code added in the transmitter. Two means are obtained from the two sets of correlation values. For first set If the co-relation value is greater than the mean ,watermark bit is ‘1’ else it is ‘0’ and for the second set If the co-relation value is greater than the mean, watermark bit is ‘0’ else it is ‘1’. The equation for correlation is given as-

$$C_r = \frac{n \sum xy - \sum x \sum y}{\sqrt{[n \sum x^2 - (\sum x)^2][n \sum y^2 - (\sum y)^2]}} \quad (4)$$

Finally, two similar watermarks are obtained in the receiver. The advantage of getting two watermarks is that we can get the information hidden from any one of the watermark even if due to various attacks one watermark is lost. Again, in most of the cases, the researchers generally considered all the blocks of the image in the transform domain. But in this paper DCT is performed only to the blocks where watermark is to be added.

C. DCT Watermarking

A DCT expresses finite number of data points in terms of sum of cosine functions oscillating at different frequencies. (DCT)-based digital image watermarking which is used for image authentication and copyright protection is the transpose method. In this method the 2 Dimensional DCT is obtained by taking two 1- dimensional DCTs in series. The image pixel value is first divided into 8x8 blocks and the row-wise 1D DCT of each block is taken. The transpose of the blocks is then determined and a column-wise 1D DCT is ascertained which gives the 2D DCT of the data. Two dimensional discrete cosine transform (2D-DCT) is defined as—

$$F(j, k) = a(j)a(k) \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} f(m, n) \cos\left[\frac{(2m+1)j\pi}{2N}\right] \cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (5)$$

$$f(m, n) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} a(j)a(k)F(j, k) \cos\left[\frac{(2m+1)j\pi}{2N}\right] \cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (6)$$

IV. EXPERIMENTS AND RESULTS

In this section, some experimental results for a low variance DCT based watermarking algorithm are shown. The algorithm is implemented in Matlab version 7.8.0.347(R2009a) with the standard [256x256] cameraman.tif image and rhinos.avi video.

The watermark is a [8x8] binary image for Image watermarking and three [8x8] binary image for video watermarking. Fig.3 and Fig.4 Represents the original image and the watermarked image. Fig.5 represents the added watermark in different portion of the image.

The various attacks performed are Gaussian filter, Salt and pepper noise, Median filter, Histogram equalization and the results are shown in Fig.8, Fig.9, Fig.10, Fig.11.



Fig. 3 Original image



Fig. 4 Watermarked image



Fig. 5 Added watermark

The PSNR value of the watermarked image with different values of modulation factor (m_k) is shown in TABLE I .

TABLE I.

Modulation factor(m_k)	PSNR value
0.5	62.5257
0.7	66.5024

Fig. 6 PSNR values for different modulation factor.

Also, PSNR values of the two extracted watermarks after different attacks are shown in TABLE II.

TABLE II.

Watermarking Attacks	WATERMARKS AND PSNR VALUES			
	Watermark image(1)	Watermark image(2)	PSNR1	PSNR2
Gaussian filter			24.0824	26.5812
Salt & pepper noise			30.1030	36.1236
Median filter			30.1236	36.1258
Histogram equalization			20.5821	26.3504

Fig. 7 Extracted watermarks and PSNR values.

The experimental results shows that the PSNR values of the extracted watermarks are very much acceptable. The various attacks performed are Gaussian filter, Salt and pepper noise, Median filter, Histogram equalization and the results are shown in Fig.8, Fig.9, Fig.10, Fig.11.

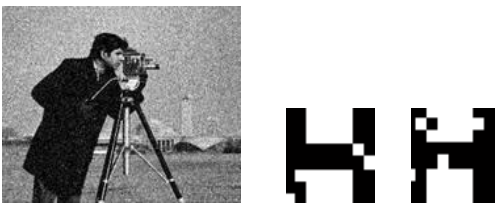


Fig. 8 Gaussian noise and extracted watermark

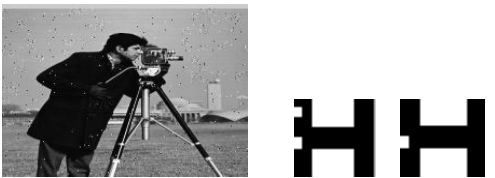


Fig. 9 Salt and Pepper noise and extracted watermark



Fig. 10 Median filter and extracted watermark



Fig. 11 Histogram equalization and extracted watermark

The algorithm is also performed with [256 x 256] colored image as well as with various frames of a video. The original image, watermarked image and extracted watermark are shown in Fig. 12(a), Fig. 12(b) and Fig. 12(c) for images and Fig. 13 is for some of original frames of a video, Fig. 14 shows the watermarks, Fig. 15 shows watermarked frames along with PSNR values and Fig. 16 represents extracted watermarks of 10 frames.



Fig. 12 a)Original image, (b) Watermarked image, modulation factor(m_k)=0.5, (c) Added watermark, (d) Extracted watermarks, (e) Watermarked image, modulation factor(m_k)= 0.7.

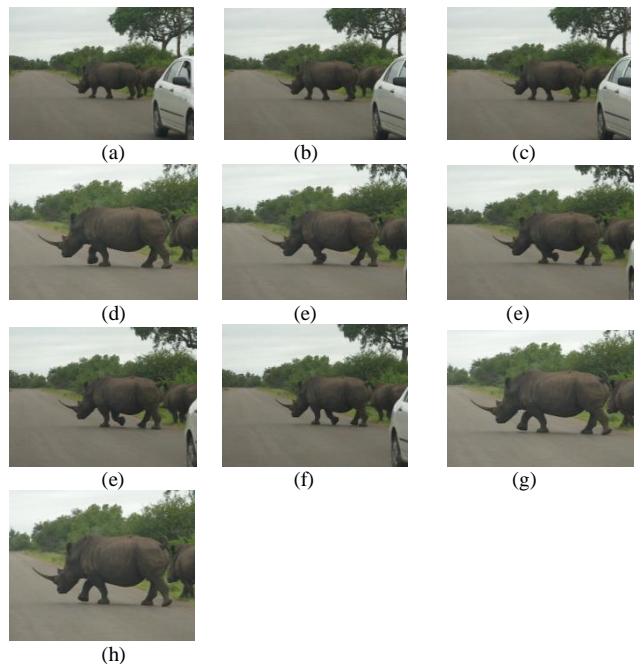


Fig. 13 Original Frames.

E C E

Fig. 14 Watermarks.

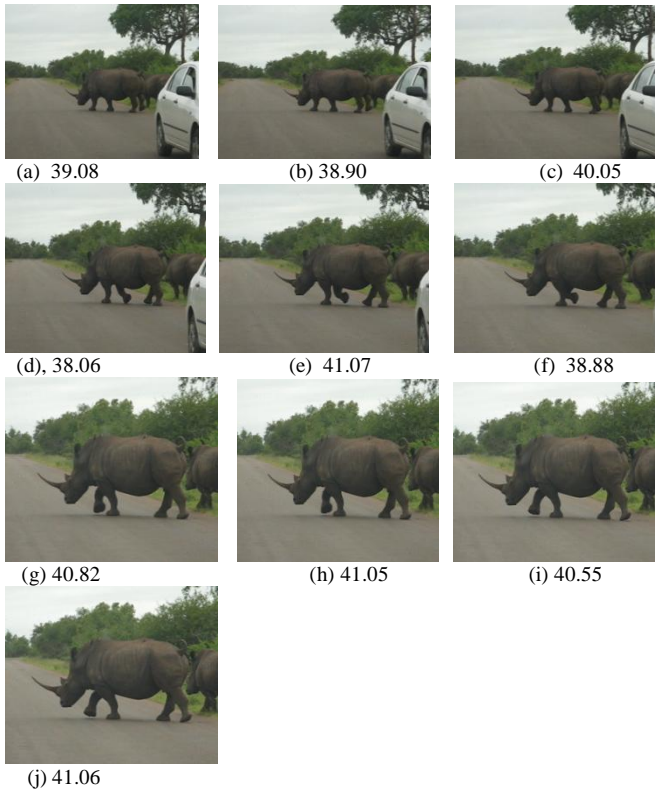


Fig. 15 Watermarked Frames, PSNR values.

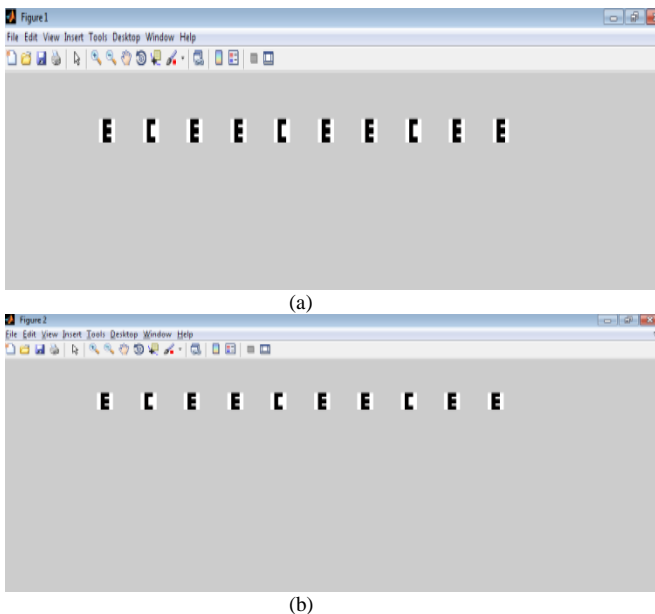


Fig. 16 Double Extracted Watermarks.

V. CONCLUSION

In this paper, the watermark algorithm is implemented based on low variance of various blocks of image and video frames. For the same watermark, it is embedded twice with gold codes, within the same randomly selected blocks equivalent to the number of bits in the watermark. Here there is no need of converting all the blocks to transform domain as a result time required for transformation of the blocks is reduced.

Also the watermark algorithm extracts two watermarks in the receiver; therefore even if the information is lost in one watermark, we can retrieve the information from the other one. As compared to other watermarking techniques it helps in finding the location of the error bit of the watermark without the help of original watermark. But, the size of the watermark must be comparatively smaller than the original image.

References

- [1] Cox IJ, Kilian J, Leighton T, Shamoon T. Secure spread spectrum watermarking for multimedia. *IEEE Trans Image Process* 1997;6(12):1673-87.
- [2] George, M., Chouinard, J.V., Georganas, N., 1999. Digital watermarking of images and video using direct sequence spread spectrum techniques. *IEEE Can. Conf. Electrical Comput. Eng.* 1 (9-12), 116-121.
- [3] T. Kohda, Y. Ookubo, and K. Shinokura, "Digital watermarking through CDMA channels using spread spectrum techniques," in *Proc. IEEE International Symposium on Spread-Spectrum Techniques and Applications*, vol. 2,
- [4] [4] R. Bangaleea, H.C.S. Rughooputh, Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterization, *IEEE 6th Africon Conference*, Vol. 1, 2002, pp. 293-298.
- [5] [5] F. Zhang, B. Xu, and X.Zhang, "Digital Image Watermarking Algorithm based on CDMA spread spectrum," in *12th International Multi-Media Modelling Conference Proceedings*, 2006, pp. 405-408.
- [6] [6] C. Bo and S. Hong, "A new robust-fragile double image watermarking algorithm," in *Multimedia and Ubiquitous Engineering*, 2009. MUE '09. Third International Conference on, 2009, pp. 153-157..
- [7] [7] Xiu-mei Wen, Wei Zhao, Fan-xing Meng "Research of a Digital Image Watermarking Algorithm Resisting Geometrical Attacks in Fourier Domain" pp: 265-268, *IEEE* 2009.
- [8] [8] Ho ATS, Shen J, Chow AKK, Woon J. Robust digital image-in-image watermarking using the fast Hadamard transform. In: *Proceedings of the international symposium on circuits and systems (ISCAS 2003)*; 2003. p. 826-9.
- [9] [9] Kutter M, Jordan F D, Bossen F, Digital signature of color images using amplitude modulation . *Storage and Retrieval for Image and Videos Dabbles* Vol. 3022, San Jose: SPIE, 1997: 518-526.