Gaussian Base Image Watermarking for Scalable Fragile Compression Attack

Bhuwan Mohan Karn[1], K Suresh[2], Ranjan Batham[3]

[1]M-Tech Research Scholar, [2]Research Guide, [3]HOD/ECE department,
Swami Vivekananda College of Technology, Bhopal, India

***Abstract*— with the increase in the digital media transfer and modification of image is very easy. This independency generate proprietorshipproblem of the user. So this paper focus on this problem of increasing the robustness of the image against various attack. Here new approach of protecting watermark of the image against for fragile images is done. Use of Gaussian function work effectively for fulfilling the requirement. Experiment is done on standard images and under compression attack. Results shows that proposed work is better as compare to previous existing research.**

Index Terms*— Color Format, *Digital Watermarking, Frequency domain, LSB.

I. INTRODUCTION

With the increase in the digital electronics era most of the work get easy, one of them is transferring of data. But this technology give rise to new problem of piracy or in other words proprietary get easily stolen. So to overcome this different techniques are used for preserving the proprietary of the owner. One of such digital approach is watermarking which is a subsection of hiding information that is used to put some information in the original image which will specify the originality of the digital data like photographs, digital music, or digital video [1, 2, 4]. One of the basic cause of the copyright issue is the ease available of the internet and some software that can modify the content as per the user requirement.

Watermark is a kind of digital data in form of text or image which can be store in the original signal. This text or image act as the owner signature in the data so that pirated and original data can be easily classify. As the pirated data do not have the original watermark which may be in form of text or image. Now watermarking technique is broadly classify into two field first is visible watermarking while other is invisible watermarking. Example of visible watermarking in figure 1 and 2 is the digital page containing logo, T.V. channel contain logo of their channel, etc.

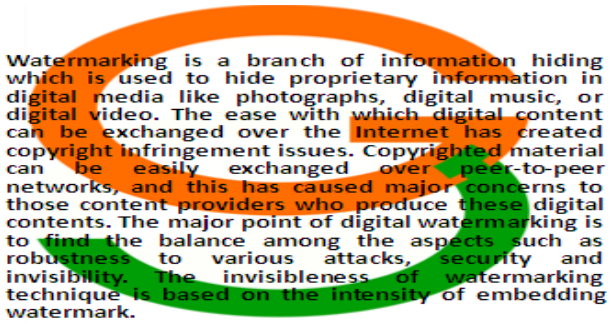


Fig. 1 Example of visible watermark in digital page.

Fig. 2 Example of visible watermark in video.

For invisible watermark use by photographer, movies, etc. who put their watermark which is invisible while it contain the watermark data either in form of text or image. Most of the watermarking techniques focus on the invisible watermarking. As embedding the watermark into the digital data is quite tough and challenge, although it is done by different methods.

II. RELATED WORK

J. Wu, and J.Xie [22] propose an adaptive watermarking technique in DCT domain using HVS model and fuzzy c-means technique (FCM). In this method FCM technique is used to classify non-overlapping 88×original blocks into categories: one is suitable for watermarking with high imperceptibility and robustness and the other is unsuitable. Watermark is inserted in DCT mid-frequency coefficients of selected blocks.

W. Zhang et el.[23] propose an adaptive digital watermarking approach. In this method FCM technique is used to determine the watermark strength of each image pixel, and then watermark is inserted adaptively to the N largest magnitude non-dc DCT coefficients of the host image. The both the method performs better against additive noise, compression and cropping etc.

YifeiPu. et el.[24] proposes a public adaptive watermark algorithm m for color images based on principal components analysis of generalizedHebb. The algorithm is based on principal component analysis of generalized Hebb adaptive algorithm in Artificial Neural Network and to do adaptive quantitative coding for principal component coefficients according to the proportion of marginal or textural information of the watermark image. In addition, it adaptively adjusts the embedding depth according to the images features to ensure the invisibility of the watermark. By way of disporting and stochastic embedding into color image watermark, it increases the embedding robustness of watermark.

C. Podilchuk, and W. Zeng [21] propose a watermarking technique for digital images that is based on utilizing visual models, which have been developed in the context of image compression. The visual model gives a direct way to determine the maximum amount of watermark signal that each portion of an image can tolerate without affecting the visual quality of the image. The watermark encoding scheme consists of a frequency decomposition based on a 88×framework followed by just noticeable difference (JND) calculation and watermark insertion. The watermark scheme is robust to different attacks such as JPEG compression, additive noise, scaling etc.

III. PROPOSED METHODOLOGY

This paper focus on the digital image invisible watermarking techniques. Then two steps are explained first is embedding and other is extraction in case of embedding digital watermark is hide in the original data such that visibility of the watermark by naked eyes is not possible. In case of extraction watermark should be successfully retrieve from the received data without any information loss of the original data as well as watermark [7, 8]. In Fig. 3 whole embedding work block diagram is explained.

Pre-Processing: Hereimage means making a matrix of the same dimension of the image then fill the matrix correspond to the pixel value of the image at the cell in the matrix. Conversion of matrix in particular format as in this work image is convert into gray format.

DWT (Discrete Wavelet Transform): Apply DWT on pre-processed image. As the image are modify in the low frequency region so the effect of compression attack is very less. If direct change is done at this level then chance of watermark recovery get decrease and quality of video also degrade as at high frequency region human can detect it easily. Here whole image is divide into four part name as LL, LH, HL, HH band where LL band is low frequency band.

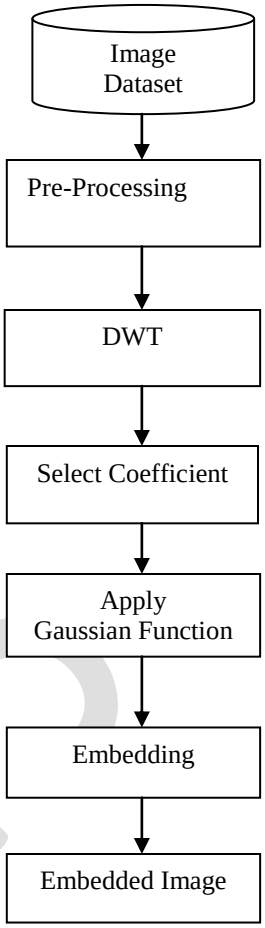


Fig. 3. Block diagram of proposed Embedding Work.

Select Coefficient: In this step each pixel value of low-low frequency band is check. Here those pixels which lay in some threshold range is consider as selected pixel for watermark hiding rest of pixels remain unaffected. Two threshold value is select let it be β and δ.

Jointly Gaussian Function: In order to increase privacy of the watermark selected pixel from above step, is randomly replace by this Gaussian function values. ConsiderGi where i=1,2,3,4,…….L and L is Gaussian random variables. It is also known as Multivariate normal cumulative distribution function if and only if each of them is a linear combination of multiple independent Gaussian random variables. Equivalently, G1 through GL are Multivariate normal cumulative distribution function if and only if any linear combination of them is also a Gaussian random variable. A vector formed by Multivariate normal cumulative distribution function variables is called a jointly Gaussian vector. For a Multivariate normal cumulative distribution function

G = |G1, . . .;GL|T , its probability density function is as follows: for any real vector g.

$$f_G(g) = \frac{1}{\sqrt{\det(K_G)(2\prod)^L}} e^{-(g-\mu G)^T K_g^{-1}(g-\mu G)/2}$$

Where μG and KG are the mean vector and covariance matrix of G, respectively.

Here $f_G(g)$ contain random values this is use for embedding the watermark pixel values.

Embedding: In this step selected coefficient least significant values are replace by Gaussian random values. Selection of number of LSB bits is also dependent on the following formula:

$$j = \max(0, \lfloor \log_2 \times \alpha \times \alpha_i \times \mathrm{mod}(f_G(g), 10) \rfloor)$$

Where α is constant to change number of selection and α_i is obtain by $f_G(g)$ /2.

Once j number of bits for hiding watermark is decide then calculate s and m values for replacement.

Compute Watermark Bit: For each coefficient Q(vi,κ,x), a sign feature s is calculate. The sign feature s is simply the sign bit of v.

if v >= 0
s= 0
Otherwise
s =1
Endif

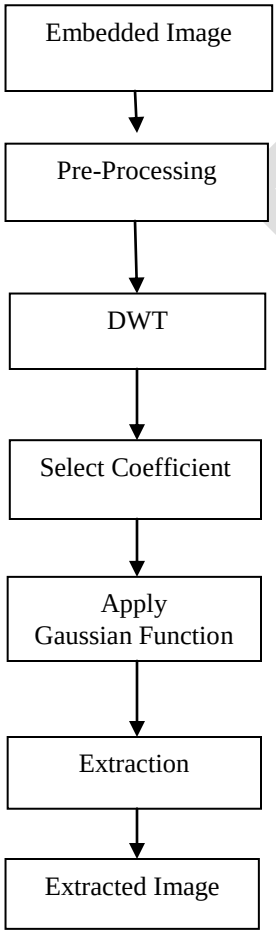


Fig. 3. Block diagram of proposed Extraction Work.

Now magnitude feature m is calculate by the quantized magnitude of coefficient values from the previous ones. This can be understand by below steps:

If Q(v,x−1)| ≤ |Q(v,x)
m= 0
Otherwise
M=1
Endif

Finally xor(s, m) for getting watermark bits that will replace selected bits from the coefficient.

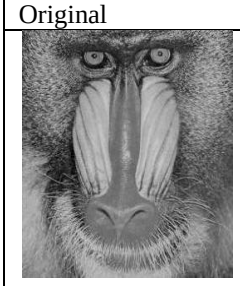
IDWT (Inverse Discrete Wavelet Transform): Finally IDWT is apply on the embedded image this will retransform the matrix in original form. This is necessary as matrix is divide as per LL, HL, LH, HH quadrants. After IDWT all the blocks are combine back to single image.

Extraction: In case of extraction all steps remain same no need of any other calculation as above xor operation will recalculate the pixel value to its original form as done in above steps. But this is possible only in case of no attack condition while in case of attack those pixel which are affected get nearby values.

IV. EXPERIMENT AND RESULT

This section presents the experimental evaluation of the proposed Embedding and Extraction technique for privacy of image. All algorithms and utility measures were implemented using the MATLAB tool. The tests were performed on an 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM, and running under Windows 7 Professional.

Dataset: Experiment done on the standard images such as mandrill, lena, pirate, etc. Result is compare at two condition first is without attack and other is at compression attack.

Original		
		

Evaluation Parameter:
Peak Signal to Noise Ratio

PSNR is use to find the amount of data present from the received signal as it may corrupt by the presence of some noise. So it is term as the peak signal to noise ratio. PSNR is the ratio between the maximum possible received information and the noise that affects the fidelity of its representation.

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Bit Error Rate:

In this parameter one can obtain the ratio of number of error bit received after the extraction to the total number of bits use for embedding. BER is zero means no error is obtain or all the watermark bits are successfully retrieve.

$$\text{BER} = \frac{Total\_Watermark\_Bit - Correct\_Watermark\_bit}{Total\_Watermark\_Bit}$$

Structural Similarity index

SSIM term is a method for finding the similarity between two images. The SSIM method use for evaluating the image quality based on an initial uncompressed or distortion-free image as reference. It is introduce to improve the traditional schemes like PSNR and MSE, which have proven to be inconsistent with human eye perception.

Extraction Rate

This is the reverse of the BER where value is obtainby the ratio of the correct bits received after extraction to the total number of bits embed at the sender. The extraction rate η is defined as follows:

$$\eta = \frac{n_c}{n_a} \times 100$$

Where*nc*is the number of correctly extracted bits, and *na*is the total number of embedded bits.

Results:

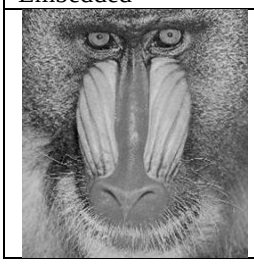
Embedded	Attacked	Extracted
		

Fig. 5. Images obtain after compression attack on embedded images.

Proposed Work Image Under Compression Attack			
Images	BER	SNR	PSNR
Mandrill	0.2412	3.2354	6.2457
Lena	0.5024	-0.1221	3.0573
Pirate	0.5182	-0.0373	2.9422

Table. 1. Proposed work results obtain after compression attack

Scalable fragile [8] Image Under compression Attack			
Images	BER	SNR	PSNR
Mandrill	0.7310	0	2.9557
Lena	0.7354	-0.1655	2.9593
Pirate	0.7426	0.2309	2.8605

Table 2.Proposed work results obtain after compression attack

From above fig. 5, table 1 and 2 it is seen that proposed method works better than previous work in [8] named as scalable fragile image. It is obtained that use of Gaussian function for randomization has increase the robustness of the image against compression, so scalable fragile image can be easily recover betterly as compare to previous one.

V. CONCLUSION

In this paper a new approach of watermarking is studied in detail. Based on human view, Low frequency band of the image is use, so here it makea invisible watermarking technique base on Gaussian function robustness of image is improve. Results shows that the proposed work is producing the results which maintain the image quality as well as

robustness against the fragile images. Watermark obtain from the extraction method is having 0.24% of BER which is quite impressive results for all the researchers. In future work can be improve for other attacks such as geometry of image. We have tried to reduce the S/N to ratio to minimum for better results and understandings. In this digital world no. of new techniques and trends are evolved and need a better algorithm and robust formulae to crack it.

REFERENCES

[1]. HaniehKhalilian, *Student Member, IEEE,* and Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DECEMBER 2013.

[2]. Walter Godoy Jr., Charles Way Hun Fung " A novel DWT-SVD video watermarking scheme using side view" 978-1-4577-1180-0/11/$26.00 ©2011 IEEE.

[3]. TamannaTabassum, S.M. Mohidul Islam "A Digital Image Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" vol. 13, no. 7, pp. 560 –576, july 2003.

[4]. Frank Hartung, Jonathan K. Su, and Bernd Girod "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks". of Multimedia Contents" International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[5]. "CHAPTER 2. WAVELET TRANSFORMS ON IMAGES"*sundoc.bibliothek.uni-halle.de/diss-online/02/03H033/t4.pdf*

[6]. Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, AnkitaTawde DIGITAL VIDEO WATERMARKING USING MODIFIED LSB AND DCT TECHNIQUE. International Journal of Research in Engineering and Technology eISSN: 2319-1163.

[7]. *Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ and Shigeo Kato* . "DIGITAL IMAGE WATERMARKING METHOD USING BETWEEN-CLASS VARIANCE". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[8]. Angela Piper1, ReihanehSafavi-Naini. "Scalable fragile watermarking for image authentication". Published in IET Information Security, on 31st December 2012

[9]. O. Bruyndonckx, J. J. Quisquater, and B. Macq, "Spatial Method for copyright labeling of digital images," in Proc. IEEE Nonlinear Signal Processing Workshop, 1995, pp. 456–459.

[10]. G. Caronni, "Assuring ownership rights for digital images," inReliable IT Systems, H. H. Breggemann and W. Gerhardt-H ¨ ackl, ¨Eds. Vieweg, Germany, 1995.

[11]. M. Schneider and S.-F. Chang, "A content-based approachto image signature generation and authentication," in Proc. ICIP'96, vol. III, pp. 227–230.

[12]. "Facsimile coding schemes and coding control functions for Group 4 facsimile apparatus for document transmission," CCITT Recommendation T.6, 1984.

[13]. M. Cooperman and S. Moskowitz, "Steganographic method and Device," U.S. Patent 5 613 004, Mar. 1997. (Available WWW: http://www.digital-watermark.com/patents.htm.)

[14]. I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread Spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997; see also Proc. ICIP'96, vol. III, pp. 243–246.

[15]. S. Craver, N. Memon, B.-L. Yeo, and M. Yeung, "Can Invisible watermarks resolve rightful ownership?" IBM Research Rep. RC20509, July 1996. (Available WWW: http://www.research.ibm.com:8080.) See also Proc. SPIE Storage and Retrieval for Image and Video Databases V, Feb. 1997, vol. 3022, pp. 310–321.

[16]. "Resolving rightful ownerships with invisible watermarking Techniques: Limitations, attacks, and implications," IBM Research Rep. RC 20755, Mar. 1997.

[17]. C. Dautzenberg and F. Boland, "Watermarking images," Dept. Of Electrical Engineering, Trinity College, Dublin, Tech. Rep., 1994.

[18]. P. Davern and M. Scott, "Fractal based image steganography," In R. Anderson, Ed., Lecture Notes in Computer Science. Tokyo, Japan: Springer, 1996, pp. 279–294.

[19]. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. IT-22, pp. 644–654, 1976.

[20]. M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," in Proc. SPIE-EI97, 1997, pp. 518–526

[21]. M. Swanson, B. Zhu, and A. Tewfik, "Object-based transparent Video watermarking," in Proc. 1997 IEEE Multimedia Signal Processing Workshop, 1997, pp. 369–374.

[22]. M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust audio Watermarking using perceptual masking," Signal Process. To be published.

[23]. M. Swanson, B. Zhu, and A. Tewfik, "Transparent robust image watermarking," in Proceedings of the IEEE International Conference on Image Processing 1996. Piscataway, NJ: IEEE Press, 1996, vol. III, pp. 211–214.

[24]. J. Tilki and A. Beex, "Encoding a hidden digital signature onto an audio signal using psychoacoustic masking," in Proc. 1996 7th Int. Conf. Sig. Proc. Appls. Tech., 1996, pp. 476–480.

[25]. R. van Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in Proceedings of ICASSP. Piscataway, NJ: IEEE Press, 1994, vol. II, pp. 86–90.

[26]. H. van Trees, Detection, Estimation, and Modulation Theory, vol. I. New York: Wiley, 1968.

[27]. A. Viterbi, CDMA Principles of Spread Spectrum communication. Tokyo, Japan: Addison-Wesley, 1995.

[28]. P. Vogel, "System for altering elements of a text file to mark Documents," U.S. Patent 5 388 194, Feb. 7, 1995.

[29]. G. Voyatzis and I. Pitas, "Applications of toralautomorphisms in image watermarking," in Proceedings of the IEEE International Conference on Image Processing 1996. Piscataway, NJ: IEEE Press, 1996, vol. II, pp. 237–240.

[30]. S. Walton, "Image authentication for a slippery new age," Dr. Dobb's J., pp. 18–26 and 82–87, Apr. 1995.

Author's Profile

Bhuwan Mohan Karn (karnbhuwan108@gmail.com) is research scholor at Swami Vivekanand College of Science & Technology Bhopal under Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal. He is Pursuing M. Tech in Digital communication. He is keen to research in different watermarking technologies and digital securities.

Prof. K. Suresh (ksureshsvcst@gmail.com) is a college guide at Swami Vivekanand College of Science & Technology Bhopal.

Prof. Ranjana Batham is HOD OF Electronics and communication department at Swami Vivekanand College of Science &Technology Bhopal.