IJRRECS/July 2014/Volume-2/Issue-7/2820-2825 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

EXPOSURE TOWARDS SECURE SYSTEM OF WATERMARKING RELYING ON SAMPLE PROJECTION

Verule Priyanka Prabhakarappa[1], SP.Chandrakanth[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

Boosting the watermarking power increases the barrier against attacks, most of the effective watermarking schemes try to match the characteristics concerning watermark to those concerning image asset. Embedding the watermark bits into the approximation Algorithm was made highly robust against noise and compression attacks by the coefficients of the image blocks. The presentation of watermarking method is analytically verified based on the performance of the introduced method via simulations on artificial signals. A novel gain invariant watermarking scheme based on a sample projection scheme was introdued. The performance of watermarking method is systematically investigated and verified by means of simulation on artificial signal. On the basis of spread spectrum a concept was introduced in which an additive watermarking concept remains very much robust against noise and cropping attacks. A novel gain invariant watermark in scheme was introduced based on a sample projection scheme. One of the common but effective attacks in watermarking systems is volumetric distortions which is the main drawback of most recent studies and even the quantization index modulation.

Keywords: Watermarking, Image blocks, Quantization index modulation, Sample projection.

1. INTRODUCTION:

Watermarking research studies mostly targets robust watermarking problems because a good watermarking scheme should always be able to deal with some attacks. To satisfy robustness against geometric attacks and reduce the watermark synchronization problem, Tang and Hang introduced a watermarking scheme which makes use of feature extraction as well as approach of image normalization [4]. On the basis of spread spectrum a concept was introduced in which an additive watermarking concept remains very much robust against noise and cropping attacks. Based on this observation that boosting the watermarking power increases the barrier against attacks, most of the effective watermarking schemes try to match the characteristics concerning watermark to those concerning image asset [8]. Based on log polar mapping (LPM) and phase correlation, Zheng introduced an image watermarking technique which embeds the watermark into the LPMs of the image Fourier magnitude spectrum. This scheme is invariant to rotation and remains comparatively robust to scaling attack. Multiplicative watermarking, as an example, has been introduced in and has been widely studied later on using local optimum decoders in multi resolution transform domains such as wavelet and contour let domains [1]. Besides, a universal optimal detector for scaling based watermarking schemes is presented. These schemes are highly robust against noise and compression attacks. Based on the specific applications Watermarking techniques are mainly categorized into three types mainly robust, fragile, and semi fragile methods. For identification purposes robust watermarking is used and for authentication applications fragile, semi fragile watermarking is usually in use [11]. Studies about the watermarking research area mostly target the robust watermarking problems while a good watermarking structure should be supposed to deal with some kinds of attacks. Based on a sample projection approach a robust image watermarking scheme was presented. For securing high robustness against attacks, usage of components concerning low frequency of image blocks in support of data hiding is practiced [3].

2. METHODOLOGY:

Digital watermarking provides information within a digital work as a component of the media. Several robust watermarking

techniques as shown in fig1 have been introduced so far. A novel gain invariant watermark in scheme was introduced based on a sample projection scheme. Embedding the watermark bits into the approximation Algorithm was made highly robust against noise and compression attacks by the coefficients of the image blocks [14]. Using an undisclosed key constructs a line segment whose slope is measured for data hiding any probable selection of four estimated coefficients which will be selected. Blind watermarking Scheme was introduced. These four samples come from approximation coefficients of the image blocks satisfying Gaussian assumption. By multiplying specific matrices to the vector samples of size four watermark embedding was done. Depending on the message symbol translation and projection of the vector samples on the already defined coding lines by the matrices [9]. By using four approximate coefficients of the image blocks which can be selected according to a secret key the introduced algorithm is useful to image signals. Against frequent watermarking attacks like angle quantization index modulation against additive white Gaussian noise, compression, and filtering various simulations showed that the introduced algorithm is highly tough [7]. The future work is going on making the algorithm tough to collision attacks. For calculating the allocation of the watermarking variable, requires Construction of a line segment in the two dimensional space requiring four samples of an independently and identically distributed estimated coefficients of the image blocks obtaining a slope invariant to the gain factor [2]. Watermarking code can be inserted by the projection of line segment on specific lines based on message bits. The presentation of watermarking method is analytically verified based on the performance of the introduced method via simulations on artificial signals [16]. Several experiments on sample images verify the efficiency of the introduced scheme in resisting against common noise attacks.

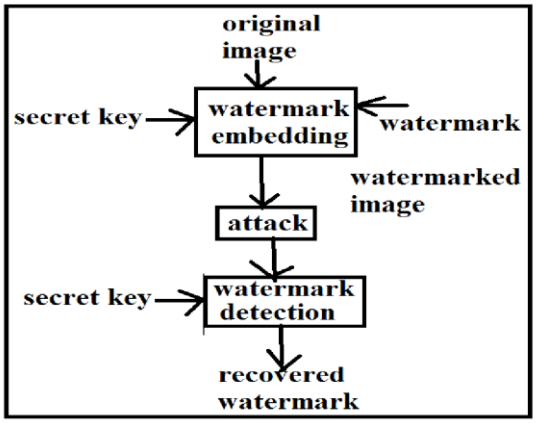

Fig1: An overview of watermarking technique

3. SOLUTIONS AGAINST ATTACKS IN WATERMARKING SYSTEMS:

One of the common but effective attacks in watermarking systems is volumetric distortions (i.e., any kind of amplitude scaling or gamma compensation). For image signals, it may happen due to scanning procedure where light is not distributed uniformly over the paper. This simple attack is the main drawback of most recent studies and even the quantization index modulation (QIM) algorithm which has attained great popularity due to its lossless effort by means of lattice-basis code books [12]. Three types of solutions can tackle this difficulty, particularly for QIM process which adopt auxiliary pilots by means of watermarked signal recognized at encoder as well as decoder by means of spherical code words with correlater decoders, or by means of employing angle QIM (AQIM) setting up a domain in which process concerning embedding is invariant to gain attack [5]. Some improvement or generalization on this scheme which is referred to as rational dither modulation (RDM) is introduced in. The first solution against the gain attack decreases the security of the algorithm, since the malicious attacker can change either the watermark or the pilot signals [10]. The main signals can be easily detected as pilots are deterministic objects. Although the second and third approach keeps the security of the QIM algorithm, they cause high computational cost. Besides, the low robustness of AQIM against additive white Gaussian noise (AWGN) and the high peak to average power ratio (PAPR) of RDM algorithm which happens due to its momentarily large quantization step size are the main drawbacks that should be addressed [6]. Thus, no approach has been presented so far that both proposes an optimal decoder and remains invariant to the gain attack. A novel gain invariant watermarking scheme based on a sample projection scheme was introdued. Embedding the watermark bits into the estimation coefficients of the image blocks makes the algorithm extremely vigorous against noise and compression attacks [13]. We entrench the watermark bits by prophetic the line segment on some specific coding lines though protecting its centre of mass. The slope of the line segment carries the watermark information although the distortion imposed to its constructive samples is negligible [12]. To put into practice the maximum detector for data extraction, we should compute the allocation

of the slope of the line segment. As the embedding process is linear, it can be indicated by multiplication of specific embedding matrices [13]. The approximation coefficients of the majority of the image blocks can be well-modelled by Gaussian distribution. The performance of watermarking method is systematically investigated and verified by means of simulation on artificial signal.

4. CONCLUSION:

Watermarking research studies mostly targets robust watermarking problems because a good watermarking scheme should always be able to deal with some attacks. On the basis of spread spectrum a concept was introduced in which an additive watermarking concept remains very much robust against noise and cropping attacks. To satisfy robustness against geometric attacks and reduce the watermark synchronization problem, a watermarking scheme was introduced which makes use of feature extraction as well as approach of image normalization. Based on the specific applications Watermarking techniques are mainly categorized into three types mainly robust, fragile, and semi fragile methods. Studies about the watermarking research area mostly target the robust watermarking problems while a good watermarking structure should be supposed to deal with some kinds of attacks. For image signals, volumetric distortions may happen due to scanning procedure where light is not distributed uniformly over the paper. Based on a sample projection approach a robust image watermarking scheme was presented. For securing high robustness against attacks, usage of components concerning low frequency of image blocks in support of data hiding is practiced. For identification purposes robust watermarking is used and for authentication applications fragile, semi fragile watermarking is usually in use.

REFERENCES:

[1] B. Chen and G. Wornell, "Quantization index modulation: a classof provably good methods for digital watermarking and informationembedding," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423 –1443,May. 2001

[2] F. Ourique, V. Licks, R. Jordan, and F. Perez-Gonzalez, "Angle qim: anovel watermark embedding scheme robust against amplitude scalingdistortions," in *Proc. IEEE Int. Conf. Acoustics, Speech, and SignalProcessing*, vol. 2, Philadelphia, PA, USA, Mar. 2005, pp. 797 – 800

[3] "Blind Image Watermarking Using a Sample Projection Approach",Mohammad Ali Akhaee, Sayed Mohammad Ebrahim Sahraeian, andCraig Jin, *2011*

[4] M. A. Akhaee, S. M. E. Sahraeian, B. Sankur, and F. Marvasti, "Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor," IEEE Trans. Multimedia, vol. 11, no. 5, pp. 822 –833, Aug. 2009.

[5] M. A. Akhaee, A. Amini, G. Ghorbani, and F. Marvasti, "A solutionto gain attack on watermarking systems: Logarithmic homogeneous rational dither modulation," in *Proc. IEEE Int. Conf. Audio, Speech,and Signal Process.*, Dallas, TX, USA, May. 2010, pp. 1050 –1053.

[6] H. Altun, A. Orsdemir, G. Sharma, and M. Bocko, "Optimal spread spectrum watermark embedding via a multistep feasibility formulation," IEEE Trans. Image Process., vol. 18, no. 2, pp. 371 – 387, Feb. 2009.

[7] J. Eggers, R. Buml, and B. Girod, "Estimation of amplitude modificationsbefore scs watermark detection," in *Proc. SPIE: SecurityWatermarking Multimedia Contents IV*, vol. 46, San Jose, Ca, USA,Jan. 2002, pp. 387–398.

[8] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "Dct-domain water- marking techniques for still images: detector performance analysis and a new structure," IEEE Trans. Image Process., vol. 9, no. 1, pp. 55 –68, Jan. 2000.

[9] J. Wang, G. Liu, Y. Dai, J. Sun, Z. Wang, and S. Lian, "Locally optimum detection for barni's multiplicative watermarking in dwt domain," Signal Process., vol. 88, no. 1, pp. 117–130, 2008.

[10] Y. Wang, J. Doherty, and R. Van Dyck, "A wavelet-based watermarkingalgorithm for ownership verification of digital images," *IEEE Trans.Image Process.*, vol. 11, no. 2, pp. 77 –88, Feb. 2002.

[11] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "Rationaldither modulation: a high-rate data-hiding method invariant to gain attacks," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3960 – 3975,Oct. 2005.

[12] S. Maity and S. Maity, "Multistage spread spectrum watermark detection technique using fuzzy logic," IEEE Signal Process. Lett., vol. 16, no. 4, pp. 245 –248, Apr. 2009.

[13] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data. a state-of-the-art overview," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 20 –46, Sep. 2000.

[14] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "A new decoder for the optimum recovery of nonadditive watermarks," IEEE Trans. Image Process., vol. 10, no. 5, pp. 755 –766, May. 2001.

[15] M. Miller, G. Doerr, and I. Cox, "Applying informed coding andembedding to design a robust high-capacity watermark," *IEEE Trans.Image Process.*, vol. 13, no. 6, pp. 792 –807, Hun. 2004.

[16] Q. Cheng and T. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," IEEE Trans. Multimedia, vol. 3, no. 3, pp. 273 –284, Sep. 2001