International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:2, 2008

A Robust Watermarking using Blind Source Separation

Anil Kumar, K. Negrat, A. M. Negrat, and Abdelsalam Almarimi

***Abstract*—**In this paper, we present a robust and secure algorithm for watermarking, the watermark is first transformed into the frequency domain using the discrete wavelet transform (DWT). Then the entire DWT coefficient except the LL (Band) discarded, these coefficients are permuted and encrypted by specific mixing. The encrypted coefficients are inserted into the most significant spectral components of the stego-image using a chaotic system. This technique makes our watermark non-vulnerable to the attack (like compression, and geometric distortion) of an active intruder, or due to noise in the transmission link.

***Keywords*—**Blind source separation (BSS), Chaotic system, Watermarking, DWT.

I. Introduction

IN the present era of computers and fast communication, one needs to protect copyright ownership from unauthorized user, through any electronic media. The private-key and the public-key are the two well-known cryptosystems [1, 2, and 3] using these we enable to keep the secret data securely in such a way that the invader cannot able to understand what the secret data means. But when the data is decrypted we cannot track its reproduction and retransmission.

For this purpose the digital watermark are used which is identification code that is permanently hidden inside the image and remain inside the image forever for identification for ownership. For more effective, the watermark should have the following characteristics:

Perceptual Transparency: The watermark should be perceptual invisible, i.e. one should not notice any degradation in the perceived quality.

Robustness: The watermark must be difficult to remove; the amount of the image distortion necessary to remove the watermark should degrade the image quality.

Universality: The same digital watermarking algorithm should apply to all three media.

Capacity: It should allow insertion of multiple, independently detectable watermark in an image.

Payload: The amount of the information that can be actually be hidden.

Unambiguousness: Retrieval of the watermark should be unambiguously to identify the owner even in the case of the attacks.

In spread spectrum communication [4], to transmit a narrowband signals over a much larger bandwidth such that the signal energy is tough to detect.

The cox's method [5] for watermarking, a sequence of values $V = v_1, v_2 ....., v_n$ which is extracted from each document D into which the watermark $X = x_1, x_2 ...., x_n$ is to be hidden and obtain the adjusted sequence $V^{'} = v_1^{'}, v_2^{'}, ..., v_n^{'}$ and which is inserted back to obtain the document $D^{'}$.

Using the equation, where α a scaling parameter.

$$v_i^{'} = v_i + \alpha x_i \quad (1)$$

Blind source separation is also used for the encryption. Blind source separation (BSS) is a technique for separating signals which we have received from the different sensors which is asset of mutually independent source signals[6, 7, 8, and 9]. It has the promising applications to communications, bio-medical engineering, ECG and EEG and feature extraction[10, 11, and 12]. The Independent component analysis (ICA) is the special case of the BSS.

The application of ICA for hiding the single image transmitted over the communication channel proposed by, Kasprzak and Cichocki [13].

Qiu-Hua Lin [14, 15] proposed image encryption, the confidential images are transmitted are covered with the mask image by specifically mixing them and on the receiving side; the original images are recovered through BSS.

The chaotic system a mechanism for generating pseudo random binary sequences [16], the pseudo random sequence is used as the key to hide watermark inside the image[17, 18].

This paper is organized as follows. In section 2, we discuss about our proposed method. In section 3, we discuss about the Experimental results and analysis. In section 4, we conclude the paper.

II. Proposed Method

To give the overview of the entire system, we will introduce the main components and their functionality, operation and data flow of each component. The proposed scheme is shown in the Fig. 1 which is composed of the embedding system, an attacking process and the detecting process.

In the embedding process, it includes the watermark; random signal generated using pseudo random sequence, a secret key using pseudo random sequence and the cover image. The watermark is decomposed into the frequency domain using the DWT and we select the LL band coefficients and permute them using the permutation function. The

permutated coefficients are specifically mixed with the random signal. Finally, the mixed signal is inserted in the cover image which is elaborated in section *C*.

In the detection process, the hidden sequence is retrieved from the cover image using the pseudo random sequence and the Blind Source Separation method.

The blind source separation is elaborated in section *A*. The pseudo-random sequence explained in section *B*. The modified hiding technique is elaborated in section *C*.

A. Blind Source Separation

Blind source separation (BSS) is a technique for separating signals from the unknown sources received at different sensors. The model for the BSS is shown in the Fig. 2. BSS employ the self-organizing learning. The noise free linear model for source separation problem has been used as follows

$$x = A * s \tag{2}$$

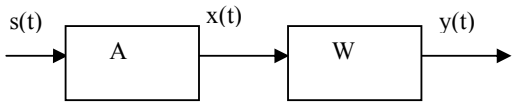

Fig. 2 Model of BSS

The vector $x = \lfloor x_1, \quad x_2, \quad ...., \quad x_n \rfloor$ is the output of the sensors. $'A'$ is the invertible $n * n$ square matrix and $s = [s_1, \quad s_2, \quad ..., \quad s_n]$ is the original source vector having the independent components, the individual source signals are assumed to have zero mean and unit variance and at the most only one them is Gaussian. The number of the sensors is equal to the number of individual sources.

To recover the individual components original source vector s , a matrix W is required , such that

$$y = W * x \tag{3}$$

where $y = [y_1, \quad y_2, \quad ....., \quad y_n]^T$ is an n-dimensional output vector. Ideally W should be equal to A^{-1}, so that $y = s$. Practically y should be close to s as possible. W is called separating matrix. These indeterminations can be further reduced if more a priori information about the sources is available.

Various approaches have been proposed for BSS. Techniques for separating mixture of sub- and super-Gaussian signals have been proposed in [14].

Algorithm: The objective function, $\psi(W)$, which is required for the separation of the signals is expressed as [15]:

$$\psi(w) = -\log|\det(w)| - \sum_{i=1}^{n} \log f_i(y_i) \tag{4}$$

Where the $f_i(y_i)$ are the marginal pdf's of the output components y_i .

On the reduction of the objective function of the above equation gives the following iterative algorithm

$$W(k+1) = W(k) + \mu(k)\left[I \quad -\phi(y(k))y^T(k)\right]W(k) \tag{5}$$

Where k denotes the time index, μ is the learning rate parameter, $\phi(y) = [\phi(y_1), \quad \phi(y_2) \quad ... \quad \phi(y_n)]^T$ is the component wise nonlinear function and the ith nonlinear function $\phi(y_i)$ is represented by

$$\phi(y_i) = \frac{\partial(\log f_i(y_i))}{\partial y_i} \tag{6}$$

When the distribution having the large tails and sharp peaks as compared to the Gaussian distribution are known as the super-Gaussian and when it's flatter than it is known as the sub-Gaussian.

In this case the entire range of the random variable is approximately taken care. This technique is useful for mixed sub- and super-Gaussian sources. Hence we can separate any unknown signals that are mixed.

B. Pseudo Random Sequence

A 1D map that exhibits complicated behavior is the logistic map from the interval [0, 1] into [0, 1], parameterized by μ:

$$g_\mu(x) = \mu x(1-x) \tag{7}$$

Where $0 \le \mu \le 4$.

As μ is varied from 0 to 4, a period doubling bifurcation occurs. In the region $\mu \in [0, \quad 3]$, the map g_μ possesses one stable fixed point. As we increase the value of the μ more than 3, the stable fixed point becomes unstable. On further increase of value of the μ , these stable periodic points in turn become unstable and each spawns two new stable periodic points of period 4.

C. Modified Watermarking Technique

Let the specifically mixed watermark with random signal is of the length 'n'. The size of the cover image is N*N, The four-level wavelet transform applied to the cover image to make the system more robust to various types of attack like compression, rotation, resizing, wiener filter, noise and cropping etc. Obtain the 'n' highest magnitude coefficients of the transformed matrix.

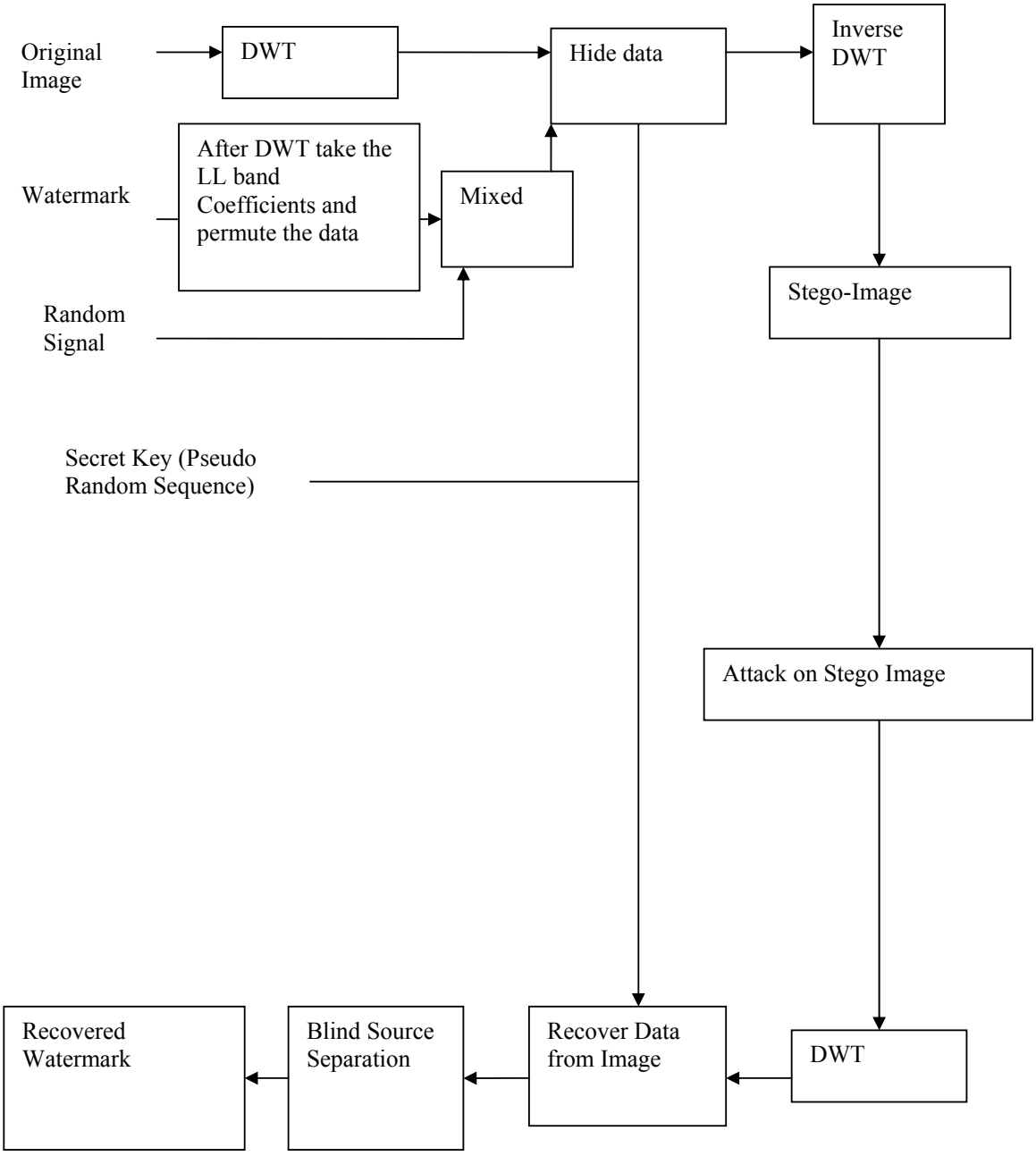

Fig. 1 The Architecture of the proposed model

The sequence of values $V = v_1, v_2 ....., v_n$ which is extracted from the cover image into which the translated and mixed watermark $X^{\mathrm{mod}} = x^{\mathrm{mod}}{}_1, x^{\mathrm{mod}}{}_2 ...., x^{\mathrm{mod}}{}_n$ is to be inserted.

The pseudo-random sequence will be generated using the chaotic system as β which will be act as the key as explained in the section *B*.

We have modified the equation (1) as

$$v_{\mathrm{mod}\,i}{}' = v_i + \alpha * \beta * x^{\mathrm{mod}}{}_i \quad (8)$$

We obtain the $V_{\mathrm{mod}}{}' = v_{\mathrm{mod}\,1}{}', v_{\mathrm{mod}\,2}{}', ..., v_{\mathrm{mod}\,n}{}'$ are the adjusted sequence and which is inserted back to obtain the document D'_{mod}. In this way we get the watermarked image.

III. Experimental Results and Performance Analysis

In our experiment we are using the Lena image of size 512*512 of true image of 24-bit color as the host image. The watermark is decomposed using the wavelet transform and permute the data using the permutation function. The permuted coefficients are encrypted using the random signal. A four-level wavelet transform applied to the cover image. We select the wavelet 10000 coefficients for embedding according to the rules of a wavelet-based HVS. We can hide at most watermark of size 200*200 of gray scale image inside the Lena image.

We perform various types of attacks on the Stego-image.

Table I, when we inserted 64*64 size image watermark in the Lena-image, and The attacks are compression of the image, rotation, rescale, histogram equalization, noise.

We are also change the value of the β sequence and it shows that the recovered data is very much distorted.

TABLE I
Performance of the Proposed Method Against Various Attacks

Attack name	*Level 4(PSNR)*
Blurring	19.2678
Contrast	24.3371
Cropping(80%)	77.3234
Dark	12.95
Deblur	38.4329
Histogram Equalization	22.34
Median Filter	18.356
Resize(50%)	47.1787
Rotation(5%)	15.7526
Weiner Filter	23.2376
Salt	17.3555
Jpeg(90%)	59.3956
Jpeg(80%)	47.9537
Jpeg(75%)	42.4356
Jpeg(50%)	39.1254
With different β	16.4739

IV. Conclusion

We have proposed the robust watermarking. The encrypted and permutated coefficients are hidden inside the image using the pseudo random sequence to increase the security of the system. This provides resistance to noise present in the channel and from any intruder. The BSS technique is suitable for mixed sub- and super-Gaussian sources. In this case the transmission is hidden from the world and more fault tolerant. Without the knowledge of the pseudorandom sequence as well as the permutation function no one will be able to extract the message.

The proposed system is flexible; it can easily modify with existing encryption methods to form dual encryption.

References

[1] J. Daemen and V.Rijmen, The Design of Rijndael, AES - Advanced Encryption Standard}, ISBN 3-540-42580-2 (Springer-Verlag Berlin Heidelberg, New York).
[2] "Data Encryption Standard (DES)," National Bureau Standards FIPS Publication 46(1977).
[3] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commun. Assoc. Comput.(1978)120-126.
[4] R.L. Pickholtz, D.L. Schilling, and L.B. Millstein, Theory of spread spectrum communication- A tutorial, IEEE trans. Commun. , 30(1982) 885-884.
[5] I. J. Cox, J. Kilian , F. Thomson, T. Shamoon , Secure Spread Spectrum Watermarking for Multimedia, IEEE trans of Image Processing, 6(12),(1997) 1673-1687.
[6] G. W. Braudaway, K. A. Magerlein , and F. C. Mintzer, Color correct digital watermarking of images, U.S. Patent 5 530759, 1996.
[7] C. S. Rai and Yogesh Singh, Source distribution models for blind source separation, Neurocomputing , 57C, (2004)501-505.
[8] C. S. Rai and Yogesh Singh, Blind source separation: a statistical approach, Neural Network World, 12 (3-4),(2003) 173-177.
[9] Yogesh Singh and C. S. Rai, Blind source separation: a unified approach, Neurocomputing, 49(1-4),(2002)435-438.
[10] A. Swindlehurst, M. Goris and B.Otterson, Some experiments with array data collected in actual urban and sub-urban environment, IEEE Workshop on Signal Processing Advances in Wireless Communication,(1997), 301-304.
[11] L. De. Lathauwer, B.De. Moor and J. Vandewalle, Fetal eletro-cardiogram extraction by source sub-space separation, Proc. HOS'95, Spain, (1995), 134-138.
[12] A. J. Bell and T. J. Sejnowskim, Edges are the 'Independent components' of natural scenes, Advances in Neural Information Processing Systems, vol. 9, (MIT Press, 1996).
[13] W. Kasprzak and A. Chichochi, Hidden image separation from incomplete image mixtures by independent component analysis, in Proc. Of the 13th Int. Conf. on Pattern Recognition, 2 , (1996).394-398
[14] Q. H. Lin and F. L. Yin, Blind source separation applied to image cryptosystems with dual encryptions, Electronics Letters, 38(19), (2002) 1092-1094.
[15] Q. H. Lin and F. L. Yin, Image cryptosystems based on blind source separation, Proc. IEEE Int. cnof. Neural networks & Signal Processing, Vol. 2, (2003) 1366-1369.
[16] C.W. Wu and N. F. Rulkov, "Studying chaos via 1-Dmaps—a tutorial," IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, pp. 707–721, 1993.
[17] Anil Kumar and Navin Rajpal, Application of T-Code, Turbo Codes and Pseudo-Random Sequence for Steganography, Journal of Computer Science 2 (2):148-153, 2006.
[18] Anil kumar and Navin Rajpal, Secret Image Sharing Using Pseudo-Random Sequence, IJCSNS International Journal of Computer Science and Network Security, Vol. 6 No.2B(2006), 185-193.