# Digital image water marking using ICA Technique

Mr R. N. Mishra,
System Engineer
Infosys Technology
E.City, Bangalore -560100
Email : rnm.mishra@gmail.com

*Abstract* - **The Internet is an excellent channel for digital assets, but copyright compliance can be a challenge. So guarding brand and intellectual property assets is essential. One of the ideas for the protection of intellectual property rights is embedding digital watermarks into multimedia data. The basic principles of watermarking methods are applying small, pseudorandom changes to the selected coefficients in the spatial or transform domain.**

**In this paper, a method based on the Independent Component Analysis technique for detection and extraction of digital image watermark is proposed. Three main issues in the design of a watermarking system were included (a) design of watermark signal to be added to host signal. (b) design of the embedding method itself that incorporates watermark signal into the host data, yielding watermarked data. (c) design of corresponding extraction method that recovers the watermark information from signal mixture using the key and with or without help of the original. With ICA techniques, it is ensured that a better-extracted watermark can be obtained. The watermark can be easily detected through Principle Component Analysis whitening process. The watermark can be further separated from the mixed sources. We evaluated the performance of the proposed method in terms of normalized correlation coefficient. Several results of experiments indicate the proposed method is remarkably effective.**

*Keywords* - **FastICA algorithm, image watermarking, information hiding.**

## I. INTRODUCTION

With the prevalence of the multimedia network, the transmission and access of digital media (such as digital images, digital video, digital audio, and so on) become more and more convenient. Though it helps people to share the information, at the same time it brings new problem to the authentication of copyright. Digital watermark is developed to solve this problem. Digital watermark is the digital signals embedded in the digital products. It may be any signal that can be used as signs or marks, such as images, letters, signs, numbers and so on. Digital watermarking, in which some information is embedded directly and imperceptibly into digital data to form the watermarked data, is one of the most effective techniques to protect digital works from piracy. The watermark (the embedded data) could be any authentication information such as company's logo, a serial number for a certain copy of document or an author signature. Once embedded, the watermark is bound to the work and it should be extractable even if the watermarked work is modified either intentionally or unintentionally. Covering many subjects such as signal processing, communication theory and Encryption, the research in digital watermark is to provide copyright protection to digital products, and to prevent and track illegal copying and transmission of them. Watermarking is embedding information, which is able to show the ownership or track copyright intrusion, into the digital image, video or audio. Its purpose determines that the watermark should be indivisible and robust to common processing and attack.

Media such as movies and images are nowadays produced and distributed digitally. It is usually simple to make copies of digital content. Consequently illegal pirate copies can be duplicated and distributed in large quantities. One way to deter authorized content receivers from illegally redistributing the media is watermarking. If individual watermarks are contained in the digital media and a receiver is a pirate and redistributes it, the pirate at the same time distributes his identity. Thus a located pirate copy can be traced back to the pirate. The watermarked media should otherwise be indistinguishable from the original media content.

*A. The foundation of Digital Watermarking*

It should be noted that the reason why digital watermarking is possible is that human vision system (HVS) is not perfect. Digital watermark utilizes the limitation of HVS to make itself invisible, thus avoiding to degrade original digital products, as well being hard to get identified or destroyed.

*B. Properties and Requirement of Digital Watermarking*

1) *Invisible*: A watermarking system is of no use if it distorts the cover image to the point of being useless, or even highly distracting. Ideally the watermarked imaged should look indistinguishable from the original even on the highest quality equipment.

2) *Robust*: The watermark should be resistant to distortion introduced during either normal use (unintentional attack), or deliberate attempts to disable or remove the watermark present (intentional or malicious attack). Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing, contrast enhancement…etc.

3) *Unambiguous*: Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack [1].

*C. What Watermarking is Used For?*

The first applications that came to mind were related to copyright protection of digital media. In the past duplicating art work was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights, artists of today can watermark their work by hiding their name within the image. Hence, the embedded watermark permits identification of the owner of the work. It is clear that this concept is also applicable to other media such as digital video and audio. Currently the unauthorized distribution of digital audio over the Internet in the MP3 format is a big problem. In this scenario digital watermarking may be useful to set up controlled audio distribution and to provide efficient means for copyright protection, usually in collaboration with international registration bodies.

In the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports.

Digital watermarking permits linking information on documents. This means that key information is written twice on the document. For instance, the name of a passport owner is normally printed in clear text. But it would also be hidden as an invisible watermark in the passport photo. If anyone tries to tamper with the passport by replacing the photo it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo.

Another application is the authentication of image content. The goal of this application is to detect any alterations and modifications in an image.

Invisible marking can be done on blank paper. Digital watermarks can also be adapted to mark white paper with the goal of authenticating the originator, verify the authenticity of the document content, or to date the document. Such applications are especially of interest for official documents, such as contracts. For example, the digital watermark can be used to embed the name of the lawyer or important information such as key monetary amounts. In the event of a dispute, the digital watermark is then read allowing authentication of key information in the contract. AlpVision developed genuine process to invisibly mark white blank paper with normal and visible ink. This patented technology is now known as Cryptoglyph.

Digital watermarking can be used for Digital Media Management. Beside applications in the fields of copyright protection, authentication and security, digital watermarks can also serve as invisible labels and content links. For example, photo development laboratories may insert a watermark into the picture to link the print to its negative. This way is very simple to find the negative for a given print. All one has to do is scan the print and extracted the information about the negative. In a completely different scenario digital watermarks may be used as a geometrical reference which may be useful for programs such as optical character recognition (OCR) software. The embedded calibration watermark may improve the detection reliability of the OCR software since it allows the determination of translation, rotation, and scaling [2].

### *D. Independent Component Analysis*

The basic principles of most watermarking methods employ the small and the pseudorandom changes to the selected coefficients in the spatial or transform domain. Most of the watermark detection schemes use some kinds of correlating detector to verify the presence of the embedded digital watermarking [3, 4].

Independent Component Analysis (ICA) was introduced several years ago as a blind source separation technique, but since then has been used in a broad range of applications, from sparse coding and denoising to feature extraction. The main assumption in ICA is that a given signal can be represented as a linear mixture of statistically independent sources. These properties combined with the simplicity of a linear mixture model have made ICA a powerful and useful tool in various research fields.

In independent component analysis, the desired representation is the one that minimizes the statistical dependence of the component of the representation. ICA was originally proposed to solve the blind source separation problem. We can recover N source signals after they are linearly mixed by an unknown matrix [5].

Applications of ICA can be found in many different areas such as audio processing, biomedical signal processing, image processing and telecommunications. ICA can be applied in digital watermark processing. In this paper, we attempt to employ the fast fixed-point algorithm, FastICA, to deal with the problem of detection and blind extraction of digital image watermark. The experimental results and the corresponding performance are also shown for watermark processing.

## II. DIGITAL WATERMARKING SCHEME

The watermark is a digital code unremovably, robustly, and imperceptibly embedded in the host data and typically contains information about origin, status, and/or destination of the data.

### *A. The Watermark Embedding Scheme using FastICA*

The basic idea in watermarking is to add a watermark signal to the host data to be watermarked such that the watermark signal is unobtrusive and secure in the signal mixture but can partly or fully be recovered from the signal mixture later on if the correct cryptographically secure key needed for recovery is used. Thus, in the generic watermark embedded scheme, the inputs to the system are the original data, the watermark and optional public or secrete key.

There are three main issues in the design of a watermarking system

a) Design of the watermark signal *W* to be added to the host signal. Typically, the watermark signal depends on key *K* and watermark information *M*, $W=f_0(M, K)$, Possibly, it may also depend on the host data ***X*** into which it is embedded, $W=f_0(M,K,X)$;

b) Design of the embedding method itself that incorporates the watermark signal W into the host data X yielding watermarked data *Y*, $Y = f_1(X,W)$ ;

c) Design of the corresponding extraction method that recovers the watermark information from the signal mixture using the key and with help the original, $I=g(X,Y,K)$ or without the original $I=g(Y,K)$. The first two issues, watermark signal design and watermark signal embedding, are often regarded as one, specifically for methods were the embedded watermark is host signal adaptive.

The watermark can be of any nature, such as a number, text, or an image. The host data may, depending on the application, be uncompressed or compressed. And secrete or public key is used to enforce security. A lot of watermark method are in fact similar and differ only in parts or single aspects of the-three topics: signal design, embedding, and recovery. Some sort of correlation methods, like a correlation or a matched filter, usually does the watermark recovery.

In this paper, we used the embedding scheme b), we obtain

$$W = X + a K + b * M \quad (1)$$

$$W = X + a K + b M \quad (2)$$

Where b is the small filter coefficients and " * " denotes convolution. Where, both the watermark M and the key K are inserted in the spatial domain of the original image X, and a and b are small weighting coefficients [6].

*B. The Scheme*

In the watermark recovery process, we adopt private watermarking system. The system contains both key and the original data for watermark detection and extraction. To assure the identification of ICA model, it is required that the number of observed linear mixture inputs is at least equal to or larger than the number of independent sources. In a general way, at least three linear mixtures of the three independent sources are needed for this system. Here, using the key means random values and with the help of the original image I, more mixed images are generated by adding them into the watermarked image W:

$$W1 = W, \quad W2=W+cK, \quad W3=W+dI \qquad (3)$$

where c and d are arbitrary real numbers.

These three images are rearranged into three rows in one matrix, to use the back ICA algorithm, which is used for de-watermarking process, and will he explained in next section.

## III. FastICA ALGORITHM

This method is based on the following two stages. Firstly, PCA whitening process for watermark detection, followed by the FastICA algorithm for watermark extraction.

*A. PCA Whitening-Watermark Detection*

If principal component analysis is used for whitening, one whitened data matrix can be computed from the formula:

$$Y=A_s^{-1/2}\ U^T R \qquad (4)$$

where $A_s$, is the diagonal matrix containing the k eigenvalues of the estimated data correlation matrix $RR^T/N$, and U is the matrix containing the respective eigenvectors in the same order. After PCA whitening, it is convenient means for estimating the number of sources or independent components, ***n***, from the rank of the diagonal matrix.

*B. FastlCA Algorithm*

After whitening, the FastICA algorithm takes following form, when the fourth-order statistics kurtosis is used:

1) Choose randomly an initial vector *w(0)* and normalize it to have a unit norm:

2) Compute the next estimation of a ICA basis vector after whitening using the fixed-point iteration rule:

$$w(k)=Y[Y^T w(k-1)]^3 - 3w(k-1) \qquad (5)$$

Normalize w(k) by dividing it by its norm, that is

$$w(k) = w(k) / \| w(k) \| \qquad (6)$$

3) If w(k) didn't converged, that is, until $| w^T(k)w(k-1) |$ is sufficiently close to 1, go back to 2).

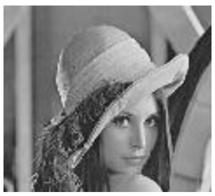
In Step 2)**,** $(.)^3$ means element-wise operation. The above procedure is the fixed-point rule for estimating one ICA basis vector. The other ICA basis vectors can be estimated sequentially if necessary by projecting a new initial basis vector *w(0)* onto the subspace which is orthogonal to the subspace spanned by the previously found ICA basis vectors, and following then the same procedure[7]. In future, with the help of multicolor channel digital watermarking method using ICA, we could demonstrate that it is possible to watermark a color image without affecting its quality.

## IV. SIMULATION RESULTS

Simulation experiments are conducted to demonstrate the validity and feasibility of the FastICA method for watermark detection and extraction. Fig. 1 shows extracted watermark from a watermarked Lena image. The performance of watermark extraction is evaluated by calculating the normalized correlation coefficient r for the extracted watermark and the original embedded watermark as

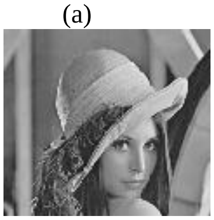
$$r = \frac{\sum_{i=1}^{L} m(i)\hat{m}(i)}{\sqrt{\sum_{i=1}^{L} m(i)^2 \sum_{i=1}^{L} \hat{m}(i)^2}} \qquad (7)$$

where $m$ and $\hat{m}$ the original and the extracted watermark sequences, respectively, with zero-mean each, and $L$ is the total number of pixels of the image .

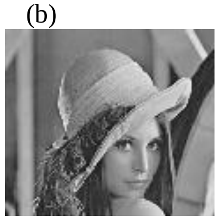


(a)

(b)



(c)



(d)

(e)

**Fig. 1** Watermark extraction results using image as the watermark (a) original Lena image, (b) watermark,
(c) watermarked image, (d) extracted Lena image.
(e) extracted watermark.

Table I shows the normalized correlation coefficients between the original and the extracted images for examples described in Fig. 1. It can be seen that the FastICA algorithm separates the images from the mixture successfully.

**TABLE I**

**PERFORMANCE EVALUATION**

| Using [7] | Test Conditions | | Correlation Coefficient, r | |
|---|---|---|---|---|
| | | 1 | Lena | Watermark |
| | | | 0.9962 | 0.9957 |
| | | 2 | Baboon | Watermark |
| | | | 0.9932 | 0.9926 |
| | | 3 | Cameraman | Watermark |
| | | | 0.9879 | 0.9941 |

The simulation results show that ICA really provides the better estimation capability.

## V. CONCLUSION

An image watermarking technique based on Independent Component Analysis (ICA) has been developed. The watermark can be detected through Principle Component Analysis and can be separated from the mixed sources by using a FastICA algorithm. The performance analysis was carried by estimating the normalized correlation coefficient, which showed that the satisfied de-watermarking performance of the approach can be obtained.

## REFERENCES


[1] Lin Liu, “A survey of Digital Image Watermarking”.

[2] F. Petitcolas, R. Anderson, and M. Kuhn, “Attacks on copyright marking systems,” in *Information Hiding* (D. Aucsmith, ed.),vol. 1525 of *Lecture Notes in Computer Science*, (Berlin), pp. 218–238, Springer- Verlag, 1998.

[3] F. Hartung and M. Kutter, “Multimedia Watermarking Techniques”, *Proceedings of the IEEE*, Vol.87, no.7, pp.1079-1107, 1999.

[4] K. Stefan and F. A. P. Petitcolas, Eds, “Information Hiding Techniques for Steganography and Signal Watermarking”, Artech House, Boston, 2000.

[5] P. Comon, “independent Component Analysis, a New Concept?**”** *Signal Process*. Vo1.36, pp.287-314**,** 1994.

[6] Minfen Shen, J. Huang, P.J. Beadle, “Application of ICA to the Digital Image Watermarking”, *Proceedings of the IEEE*, pp.1485-1488, 2003.

[7] A. Hyvarinen and E.Oja, “A Fast-fixed Point Algorithm for

Independent Component Analysis”, *Neural Computation*, pp. 1483-1492, 1997.

[8] Hanane H.Mirza, Hien D. Thai and Zensho Nakao, “Multi-color channel video watermarking”, Bult. Faculty of Engineering, Univ. of the Ryukyus No.69, pp 65-69, 2008.


* * *