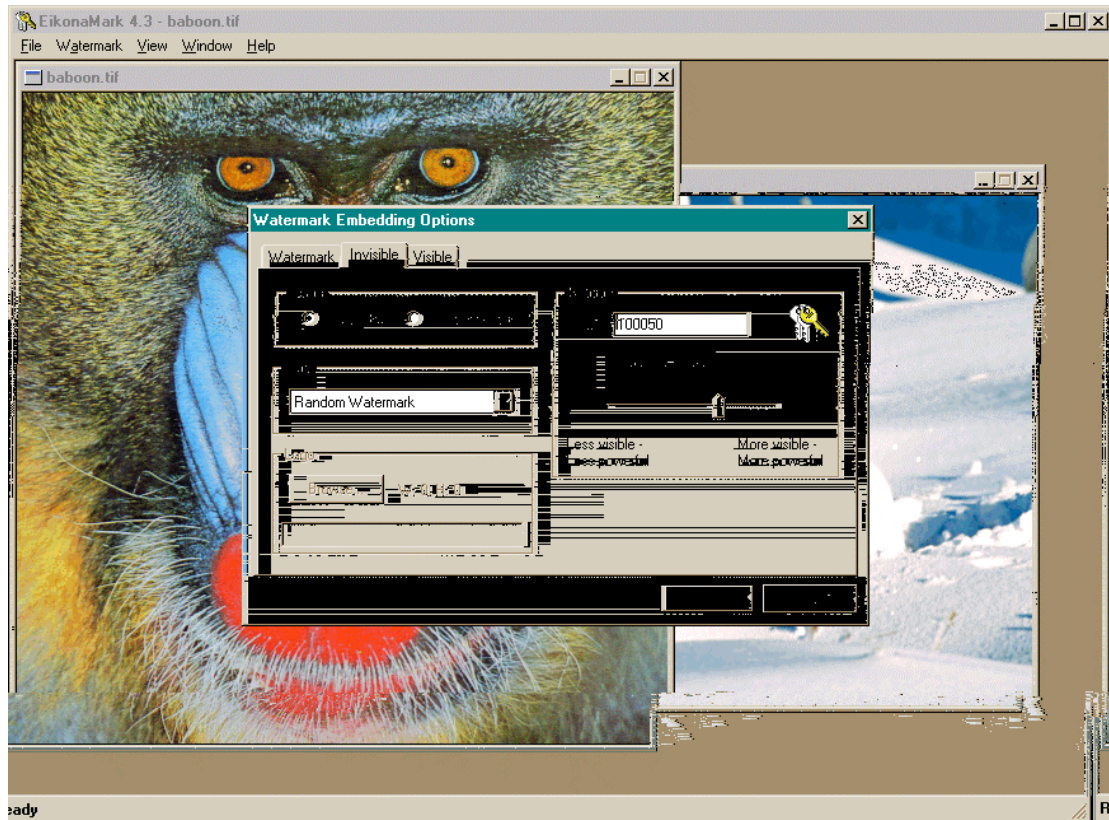


# EIKONAMARK

## Software Package for Digital Image Copyright Protection & Authentication

Version 4.3



*Overview / User's Guide*

## Contents

Version 4.3 .....	1
<b>Contents</b> .....	2
<b>Introduction</b> .....	3
<b>Features</b> .....	3
Watermark operations .....	3
Implementation.....	4
Multiple file operations .....	5
<b>User Interface</b> .....	5
Menu Commands .....	5
File Menu .....	5
Watermark menu .....	6
View menu .....	7
Window menu .....	7
Help menu .....	7
Procedures .....	8
Embedding .....	8
Detection .....	12
Batch Processing .....	13
<b>System Requirements</b> .....	14

## Introduction

*EikonaMark* is a powerful and flexible software for casting and detecting watermarks (signatures) on digital images, either color or grayscale. It can be used either for copyright protection or for authentication and tamper proofing of digital images. A copyright owner can cast its unique id number (or any identification information) as a watermark on any digital image. Watermark detection is used either for detecting if a given watermark (owner's watermark) is embedded in the test image or for detecting the image tampered regions (image authentication). The results of watermark detection can be used either for security applications or as legal proofs.

## Features

### ***Watermark operations***

EikonaMark version 4.3 includes two separate methods for copyright protection and authentication. The first method incorporates invisible watermarks, which use imperceptible digital information embedded in any kind of digital images. This method is referred to as ***Invisible Watermark***. Watermark detection in a suspected image is performed without the need of the original image.

The watermarking method for copyright protection is robust against lossy image compression (e.g. JPEG up to 30:1 with strong embedding), image filtering (e.g. mean, median) and other image processing operations (e.g. histogram equalization). The watermarking method has the additional feature of being robust against geometric distortions of the original image. Moreover the method is robust against rotation, scaling and cropping of the original image. Robustness is achieved by using watermarks having a specific structure and fast algorithms for searching the watermark in the image. The rotation searching needed for an image of 512x512 is from 0 to 22 degrees rotation. If the image is smaller the searching region must be increased. The search region should also be increased for cropped images or images that have suffered heavy image processing operations.

Binary image logo scrambling can be also used for generating the watermark. In that case the watermark is not robust against geometric distortions. In the watermark detection the encrypted logo can be recovered from the image.

The watermarking method for image authentication can detect malicious or innocuous attacks to the watermarked image. In the watermark detection the watermark detection ratio is calculated and it should be  $>0.99$  for an image that has not been tampered. The method is robust against high quality lossy image compression. In that case the watermark detection ratio is reduced and an automatic technique is provided for discriminating between alterations caused by lossy compression and malicious image editing. The method provides the used with an image map that highlights the tampered image regions.

The second method that is used for copyright protection incorporates *visible watermarks*, which use a logo image as identification embedded in an image. This casting method produces an image which has a visible (controlling the parameters of coverage and strength) logo “stamped” on the original image. The power of protection of this method depends on the difficulty to extract the logo from the original image. The logo is embedded in such a way that any attempt to extract the logo should lead into a flaw image. Such a method could be useful in TV & Video production and broadcasting.

### **Implementation**

EikonaMark is a multiple document interface (MDI) Windows (Win32 architecture) application. It is totally coded in C++ programming language making extensive use of MFC libraries. All operations are executed through menu commands and dialogs which extends the user-friendliness of the program. Each digital image is displayed as an independent window frame (document) inside the application's workspace. A casting or detection operation is executed on the currently active document.

## Multiple file operations

EikonaMark can perform *batch processing* file operations. The user can embed or detect a whole set of images that reside in a selected directory using the same operation options.

# User Interface

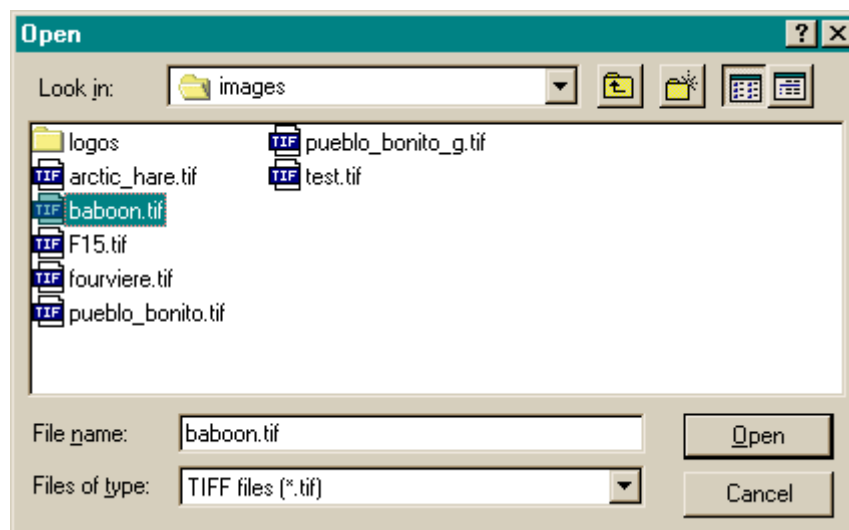
## Menu Commands

### File Menu

- **Open command:**

Loads an image to application's workspace from a file in disk.

Executing this command will show up the file open dialog from which navigation to the file system and selection of the desired file can be performed. EikonaMark supports the following file formats: TIFF (\*.tif), Windows BMP (\*.bmp), JPEG (\*.jpg), GIF (\*.gif) and TARGA (\*.tga).



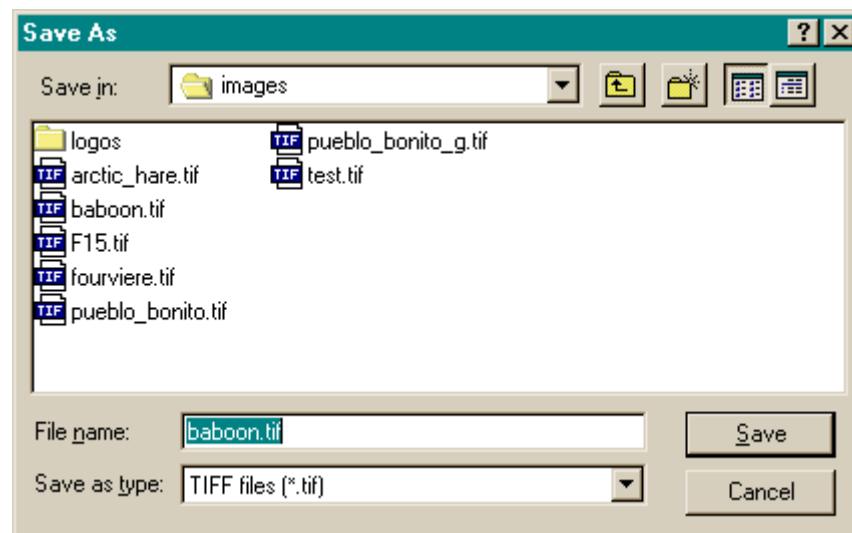
- **Close command:**

Closes the active document.

- **Save As command:**

Saves the active document to file in disk.

Executing will show up the file save dialog from which navigation to the file system is performed. EikonaMark supports the following formats on saving: TIFF (\*.tif), JPEG (\*.jpg) and TARGA (\*.tga).



- **Batch command:**

This command will start-up the batch processing dialog. More details on the batch processing capabilities on the “Procedures” section.

- **Recent file list:**

The recent file list is the name of the files most recently used. EikonaMark will hold the 4 most recently used files for easy access.

- **Exit command:**

Quits the application.

## Watermark menu

- **Embed command:**

Executes the embedding options dialog from which you can select the options for the embedding operation. Acceptance of these will perform the embedding on the



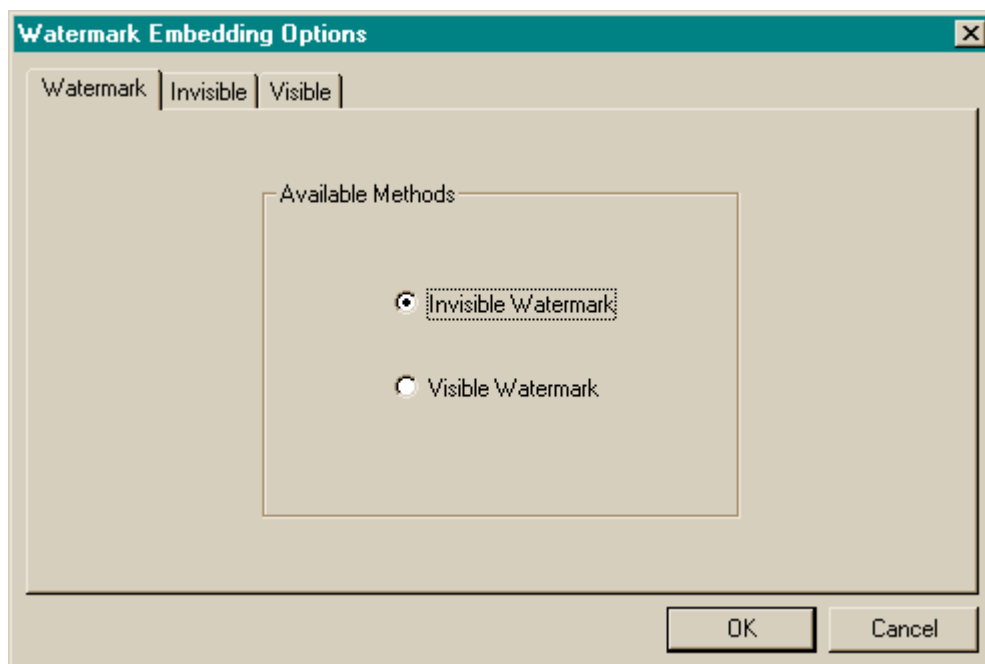
Shows up the about dialog which displays information about the application. Contact information is included on the dialog. The user can visit the company's web site and/or send an e-mail by clicking on the appropriate links.



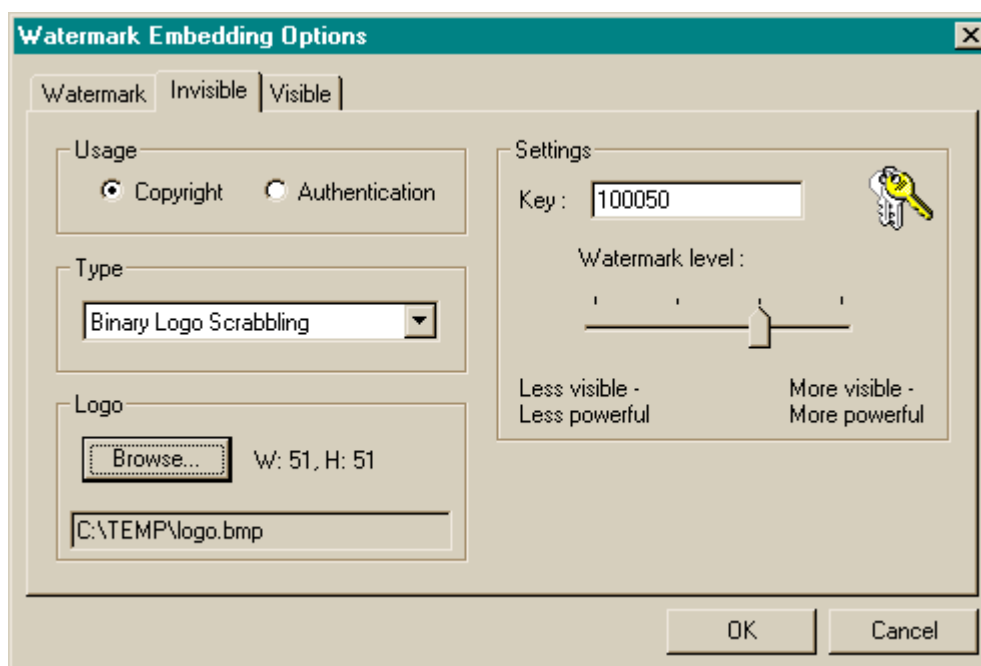
## Procedures

### Embedding

The **Watermark->Embed** command will show up the **Embedding Options** dialog. The **Watermark tab** on this dialog permits the selection one of the two methods available, either the **invisible or visible watermark**. The selected operation is the one that will be performed.



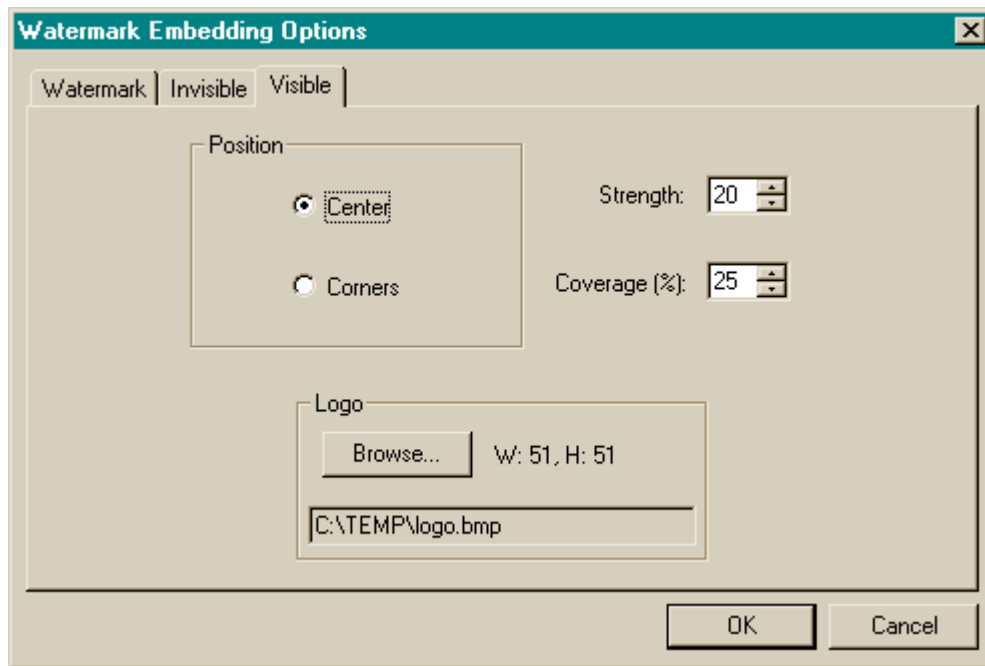
The *Invisible tab* will show up the options concerning the invisible watermark method. The user can select the usage of the embedding, either in copyright mode or authentication mode. The *copyright mode* is used when the user wants to protect the image against transformations (e.g. compression, filtering) and distortions (e.g. rotation, scaling). The *authentication mode* is used when the user wants to protect the image against malicious or innocuous attacks.



Under copyright mode the user can select the type of watermark, which can be one of the two available in the *Type box* (Random Watermark or Binary Logo Scrambling). *Random Watermark* embeds a random watermark, which is generated according to the entered key and the image characteristics, in the image. When the user selects the *Binary Logo Scrambling* option a logo image file must be selected in the *Logo box*. The *Logo image* must be a bilevel image and the number of pixel on the logo must not exceed the 10% of the number of pixels of the active image. The key must be entered in the *Key edit box*. In this version of EikonaMark the key range is limited to 100 keys, from 100000 to 100100. Finally, the user can select the watermark embedding power using the *Watermark Level* slider. There are four power levels. The first level is the one that has no or minimal effect on the visual perception of the image concerning the human eye, the fourth level is the strongest and in some cases might be visible. The following picture shows two images, the first is the original and the second is the watermarked image. The type of watermark used is random watermark with

third embedding power level. As it can be observed the user discriminates between the original and the casted image with great difficulty.

The **Visible tab** will show the visible watermark options. The options include the position of the logo, the strength, the coverage and the logo image. **Logo** can be placed either on the center of the image or on the four corners. The **strength option** determines the visibility and takes values from 0 to 255 (greyscale levels). The default value is 20. The **coverage option** determines the percentage of the image that the logo will cover. The default value is 15% when the position is set to corners and 25% when the position is set to center. The logo image must be a bilevel image.



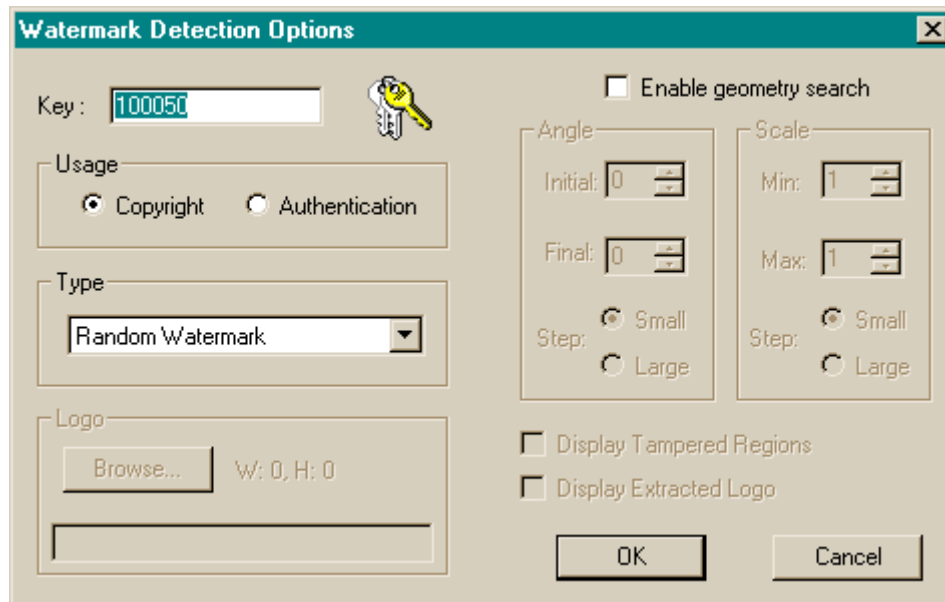
The following picture shows an image embedded with the visible watermark method using the center position, strength 20 and coverage 25%. The user can easily discriminate the logo used.



When an image signed the title of the image document will have the "- Signed" suffix.

## Detection

The procedure is launched from the **Watermark->Detect** command. It will show up the **Detection Options** dialog.



It is noted that the detection procedure applies only to images that have been casted with the invisible watermark method.

The watermark detection dialog box is comprised of the options that define the watermarking method and the type of the watermark (as in the watermark embedding dialog) and some additional options that will be described below.

In copyright mode and binary scrambling watermark the user can check the **Display Extracted Logo** option. With this option on, the application will display the logo that is extracted from the test image. The quality of the extracted logo depends on the distortions of the watermarked image.

In authentication mode the user can check the **Display Tampered Regions** option. Having this option checked the application would display the image regions that have been altered or attacked.

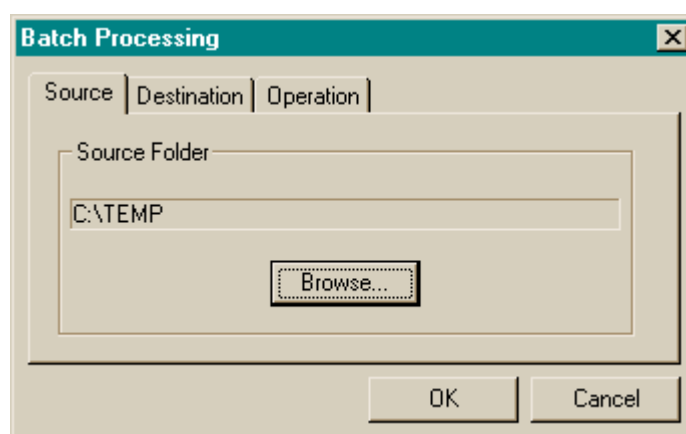
In copyright mode and random watermark the user can select the **Enable Geometry Search** which will instruct the application to perform watermark search for geometric distortions (rotation and scaling) of the test image. The user can select the initial search angle (-179 to 0 degrees), the final search angle (0 to 180 degrees) and the search step which can be either **Small** (1 degree) or **Large** 2 degrees. Moreover, the

user can select the minimum search scale (0.1 to 1), the maximum search scale (1.0 to 50.0) and the scale step if the test image is scaled. The scale factors are applied to the test image. That is, if the test image is scaled by a factor of 1.2 then in the detection dialog the minimum scale search should be 0.82.

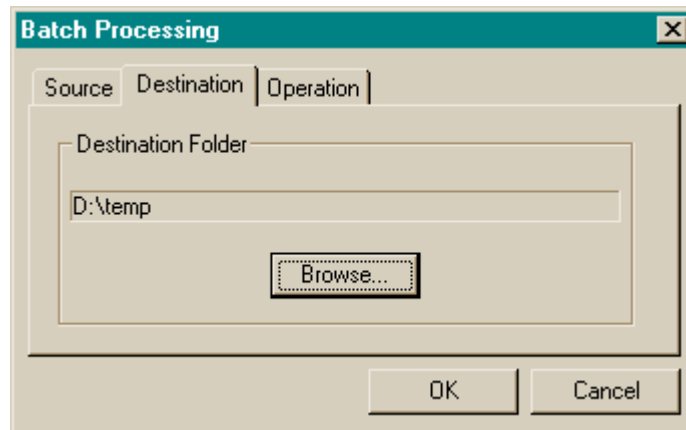
In copyright mode a message will inform the user whether the watermarked was detected or not. In authentication mode a message will inform the user about the watermark detection ratio found in the image. This detection ratio corresponds to the percentage of the watermarked pixels that were correctly detected.

## Batch Processing

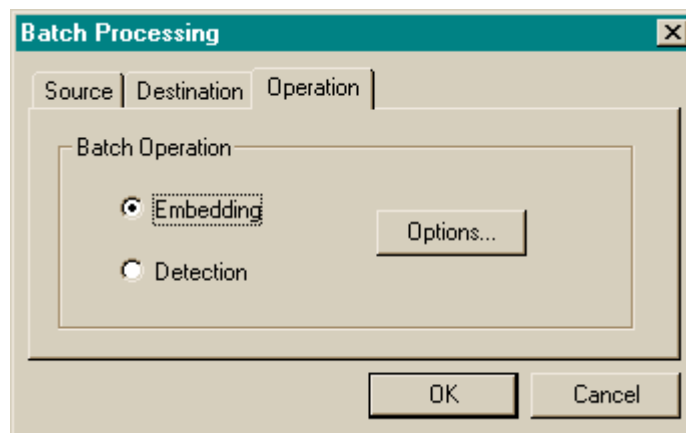
The **File->Batch** command will show up the **Batch Processing** dialog. Batch processing will perform either watermark embedding or detection procedures on a number of images. The image files that will be used should be located on the same directory, the **Source Folder**. This directory can be selected on the Source tab using the Browse function. Batch procedure will scan the directory and will load all the image files that are located in this directory (based on the supported image formats).



If the operation to be performed is embedding the user must select the destination directory where the signed images will be written. The signed files will have the same name as the originals plus the suffix “\_signed”. Moreover, all the signed files will be written using the TIFF format. In brief, an image loaded during the batch watermark embedding procedure named ‘image1.bmp’ will be stored as ‘image1\_signed.tif’. The destination directory can be selected by the browse function.



The user can select the operation that the batch procedure will perform, either embedding or detection, using the operation tab. The *Options* button will show up the corresponding dialog. The settings will remain the same for all images. At the end of the batch detection operation a log file will be written in the source directory named 'detect.log'. This file contains information about the watermark detection result of each tested image. This file will be automatically opened using Notepad.exe.



## System Requirements

EikonaMark 4.3 is a 32-bit Windows application. One of the Windows 9.x, Windows NT 4.0, Windows 2000 operating systems is needed to execute the application. The minimum hardware requirements are:

- Entry level PC, with an Intel Pentium processor or compatible.
- 64 MB RAM
- 16 bit color depth

EikonaMark is distributed as one executable named eikmark.exe.

Alphatec Ltd. Copyright © 2000