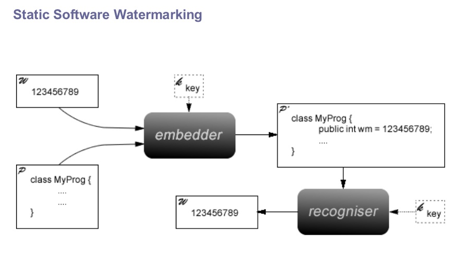
**Software Development Protection Techniques**

**Code obfuscation.**

Code obfuscation : is a set of program transformations that make program code and/or program execution difficult to analyze, and it can hide certain properties such as a software fingerprint or a watermark , In the case of obfuscation, the ‘key’ can specify which transformations were performed, in what order, and on which section of the code. This key allows the software owner to reconstruct the code , These keys can be kept in a database until required for maintenance or analysis of bug reports.

* **Watermarking** )Code obfuscation(:
* Static watermarking:



It’s a technique that adds obfuscation to program code .

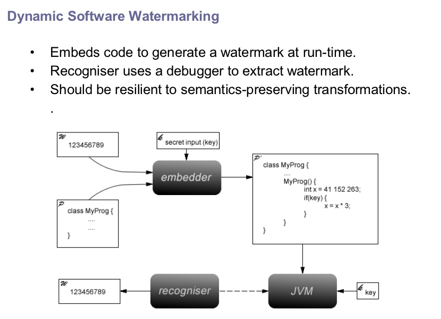
1 - adding redundant syntax to the program in which makes it more complex to understand (spaghetti code) , but doesn’t change the logic, in addition, an ambiguous part of code could be added to prove the ownership of the author (it’s like a puzzle , solving it leads to a surprise).

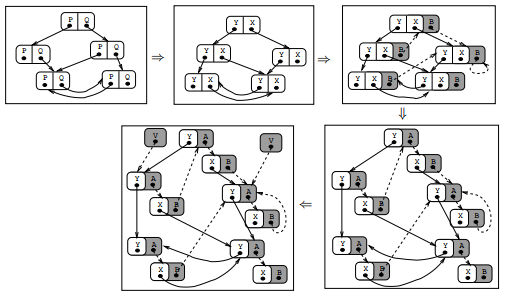
2- reordering the program blocks to make the program flow more complex to understand, but doesn’t change the logic, in addition false branches could be added.

3- renaming the variable names to make it more ambiguous.

4 – “Essential” parts of the program are steganographically encoded into the media. If the watermarked image is attacked, the embedded code will crash.

* Dynamic watermarking:





The obfuscation depends on the input (i.e. false branches are not static )

It changes the program flow depending on the program input at the run time unlike the static , but keeping the same logic .

**References:**

[1] <http://softeng.polito.it/events/watermarking.pdf>

[2] <https://www.slideshare.net/j_ham3/static-software-watermark>

[3] <https://www.esat.kuleuven.be/cosic/publications/thesis-199.pdf>