



## TECHNOLOGY

Founded upon our patented microparticle technology, we have created a comprehensive and practical suite of authentication solutions that are impossible to compromise.

There are three major technological components in every security solution we design:

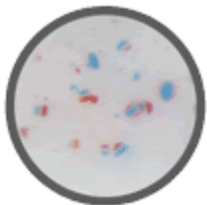
- **Stealth Mark<sup>®</sup> Marks & Codes** – the physical, microparticle mark which is applied to an item, and the numeric code derived from those particles within the mark that is used to authenticate the item.
- **The StealthFire<sup>™</sup> Reader** – a powerful handheld device used to capture a mark image and stream it to StealthFire<sup>™</sup> software for analysis.
- **Our StealthFire<sup>™</sup> Software** – our proprietary software suite consisting of both PC and Web based applications.

## TECHNOLOGY

### Stealth Mark<sup>®</sup> Marks and Codes

What makes our marking so unique? Let's break it down.

First off, each mark is comprised of a variable number of our proprietary microparticles. Each microparticle is made up of a variable number of layers. And each layer will vary among a proprietary set of colors.



Second, because our microparticles are as small as 5 microns (a human hair is approximately 80 microns), you can't see it with the naked eye. This means that a potential counterfeiter or diverter doesn't even know that you are protecting your product.

Third, by varying the number of microparticles, the number of layers within the particle, the colors, and using our patented encryption algorithms, we design each mark to create a unique numeric code, which is licensed to a customer for their exclusive use.

Finally, because the encrypted microparticles are dispersed in a way which creates a random pattern when the mark is physically applied to an item, we can capture the characteristics of how the encrypted microparticles are dispersed in an "expression matrix." And with the combination of the encrypted code and the expression matrix, we produce a mark which is as unique to each



item as a fingerprint is to each human – a particle fingerprint. With this type of “simple complexity”, a Stealth Mark<sup>®</sup> particle fingerprint is impossible to compromise.

Further, our particle marks are:

- Nontoxic.
- Heat, chemical and crush resistant – They can survive explosions.
- Not mechanical or electrical and cannot break down. They are not subject to cyber attacks (i.e., “hacking”) like RFID tags are. Yet, they can be coded to carry intelligence.
- Well-suited for use in covert applications.
- Far more affordable and cost effective than competitive technologies such as holograms, DNA strands, or RFID.

## **TECHNOLOGY**

### **Levels of Protection**

Our security technology provides the ability to choose between two levels of protection, the standard Stealth Mark<sup>®</sup> codes or the Stealth Mark<sup>®</sup> particle fingerprint. The same mark and application methods can be used with either level of protection. Using a StealthFire<sup>™</sup> Reader, the image is taken of a mark on an item and instantly uploaded into our StealthFire<sup>™</sup> software. The software can then calculate and display the code. If you've opted for the higher level of security, it calculates the particle fingerprint and matches it to your customer database for authenticity.

### **Codes**

Codes are recognized and displayed to the user by capturing an image of a mark, via a StealthFire<sup>™</sup> Reader, which in turn, live-streams the image data to a PC with StealthFire<sup>™</sup> software. The software quickly analyses the mark and returns the code.

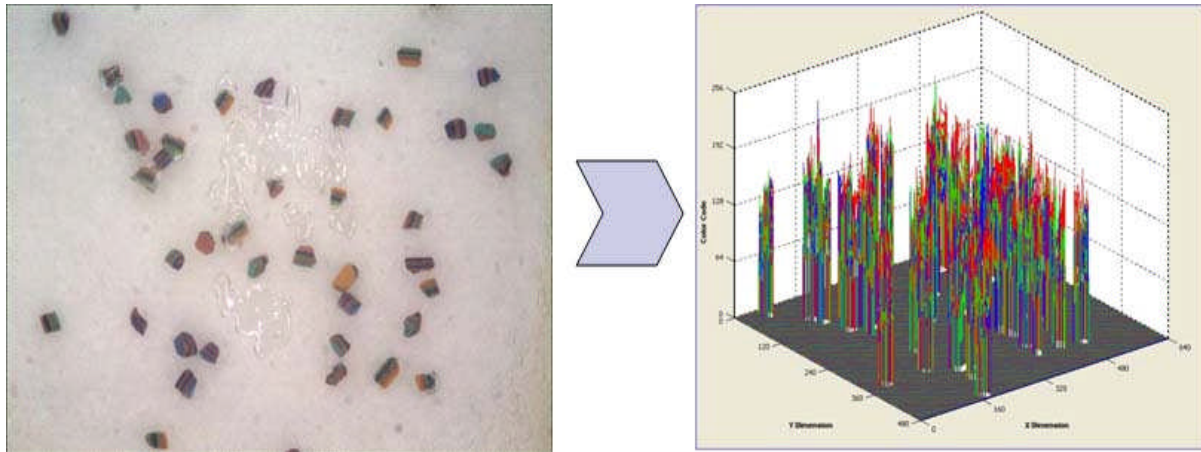
The StealthFire<sup>™</sup> software analysis separates the microparticles in the mark from their background, makes corrections for the environment in which the mark is located (enabling effective code determinations on many different colored surfaces), identifies the color of the layers in each microparticle and calculates the code. All of this occurs automatically and results are presented within a few seconds of the capture of the mark.



# Stealth Mark



Later, when your item needs to be authenticated, a new image of the mark is captured, the Code and the “Expression Matrix” are computed and the data is matched against all of the microparticle fingerprint data stored in your database to authenticate the individual item. Our process matches your particle fingerprint on more criteria than are used for human fingerprints. This verification process is similar in nature to validating a credit card and can be performed virtually anywhere. The chart below shows a mark image and a graphical representation of the Stealth Mark<sup>®</sup> fingerprint data.



## TECHNOLOGY

### StealthFire™ Reader

The StealthFire™ Reader is an optical device custom designed and fabricated to capture a mark image and live-stream it into our PC-based StealthFire™ software. The Reader provides the interface between the physical mark and the software used to compute the code and provide validation of a microparticle fingerprint.



Our StealthFire™ Reader features include:



- Capture and transmittal of image data from any Stealth Mark<sup>®</sup> security marks.
- Portability. A handheld unit, it can be used equally well in either the lab or field.
- Industrial build quality, in a unit about the size of a TV remote.
- Programmable capability for use in specific applications.
- The ability to connect to any portable PC (running StealthFire software) via USB 2.0.
- Easy adaptility for installation on production lines

## **TECHNOLOGY**

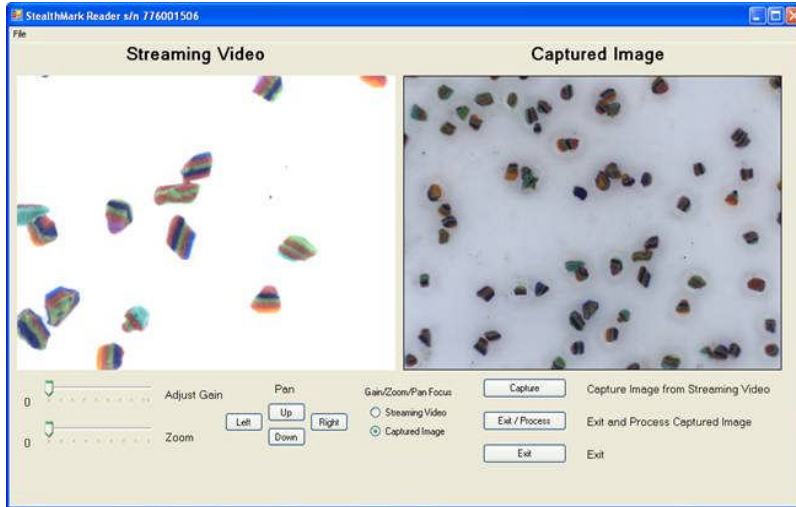
### **StealthFire™ Software**

Our suite of proprietary software applications. The software provides the backbone of the system by receiving image data from the StealthFire™ reader and analyzing that data to provide the user with the represented code.

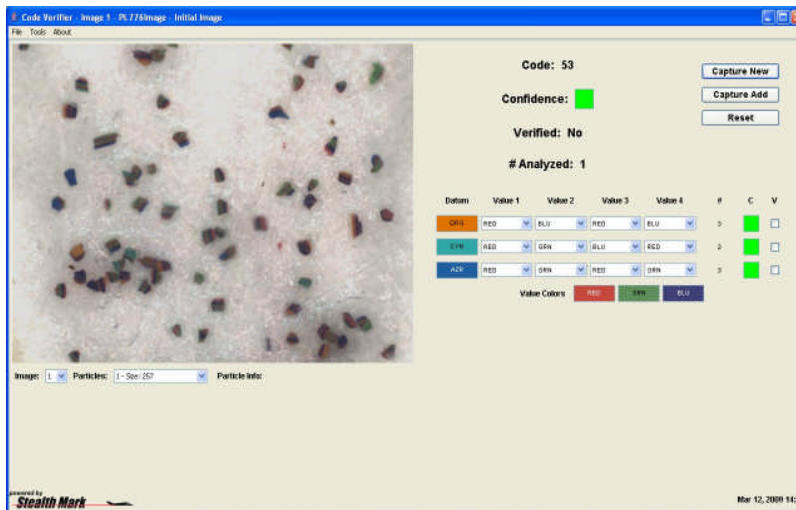
Components of the StealthFire™ software suite reside both on Stealth Mark's secure web servers and on customers' PCs. Our software has been designed and tested to provide forensic level support to the Stealth Mark<sup>®</sup> authentication technologies. The functionality of the StealthFire™ suite includes:

- Capturing mark image data (via a reader) and processing the data to display the represented code.
- Manual verification and forensic support of a reported code if desired.
- Capturing and processing a microparticle fingerprint.
- Manual verification and forensic support of a microparticle fingerprint if desired.
- Calibration, tracking and security of the reader.
- Maintaining the list of the codes assigned to a Company and the products they are related to.
- Maintaining a database of microparticle fingerprints.
- Integration with customers ERP systems or other databases.
- Various administrator functions, such as adding and deleting users, upgrading software versions, upgrading reader parameters, etc.

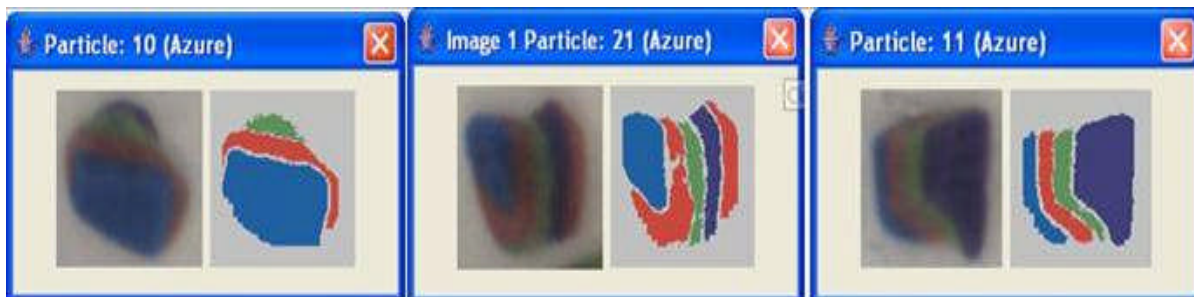
## **IMAGE CAPTURE**



## CODE CALCULATION



## INDIVIDUAL PARTICLE ANALYSIS





## IMAGE ANALYSIS

The StealthFire™ image analysis process is basically one of separating “signal” from “noise” in the image. These 3-D Pixel Graphs below plot color values versus XY location. The graph below depicts the image of a mark prior to analytical processing. The graph on the right depicts the image of a code after processing.

