

Combining Nanocharacter Printing, Digital Watermarking and UV Coded Taggents for Optimal Machine-Readable Security

George K. Phillips

Verify First Technologies, P.O. Box 7001, Paso Robles, CA 93447 USA

ABSTRACT

The ability to combine printed encrypted nano/micro structures and nano alpha/numeric algorithms – ‘NaNOcopy™’/‘LogoDot™’ – with embedded digital hidden data, - ‘digital watermark’ – and/or coded UV taggents – TechMark™ to create the ultimate machine readable Lock - Hide a Key - Key protection for documents or packaging security is new.

Extreme minute nano characters, structures, photographs, or logos, can be printed on a document in a specific pattern configured for forming an anti-copy latent warning message, which appears when copied. The NaNOcopy™ structures or LogoDots™ are uniquely micro printed to formulate certain encrypted information or algorithm calculation for further verification and protection from counterfeiting or alteration.

Major companies such as IBM, Xerox, Digimark and Spectra Systems are presently offering digital watermarking technologies to secure both digital and analog content. Appleton Security Products has a VeriCam™ hand held reader, which can detect the combination of a substrate embedded UV coded taggent, TechMark™, with the presence of other data such as a digital watermark and NaNOcopy™/LogoDot™ printing. Unless the reader identifies the presence of the TechMark™ UV coded taggents, the data carrier cannot be opened.

Keywords: Digital Watermarking, UV Coded Taggents, NaNOcopy™, LogoDot™, TechMark™, VeriCam™ Machine-Readable Security

1. INTRODUCTION

Over the past ten to twelve years, there have been many introductions of anti-fraud technologies to both protect a product/document from counterfeiting or digital replication, and to help provide for easy verification of authenticity. Many of these developments are unsuccessful due to either their design limitations or, more often, to the psychological human nature to resist FIRST LINE INSPECTION techniques; i.e. to take the time to closely inspect for image complexity and traditional anti-fraud features such as micro printing or watermarking. This becomes especially true when the recipient is under time pressure or uninformed of proper inspection analyses. Consequently, unless training on traditional accepted security technologies is given with the understanding that the person must be given enough time to give a thorough FIRST LINE INSPECTION, the probability for success is not likely. To overcome this human senses phenomenon one must more closely evaluate why most FIRST LINE INSPECTION features fail. Possibly the greatest reason is lack of awareness and perception of value of a product or document to prompt an individual to more closely analyze for genuineness. An individual who has awareness of the value through optically visualizing specific design features or ergonomics will be prompted to take action and further investigate for originality. We can refer to this as a “call to action” phenomenon. A good illustration of this “call to action” phenomenon would be that most Americans are aware of the security features incorporated into the US currency because the US government has done a good job of alerting us of the currency security features. So the US currency, as well as other currencies, has a built in human sensory factor to “call to action” or inspection. Other documents may be printed to stimulate a “call to action” by printing in high end guilloche geometrical patterns with prismatic printing and micro text or latent images, but are too complex for anyone except a subject matter expert to properly evaluate. A modern digital colored copy of such a sophisticated document would probably go unnoticed by the average person. Intricate production processes do not guarantee the integrity of a document if the applied security features can be imitated successfully, and with relative ease, without the need for the original high-grade production methods. Consequently, the (seeming) presence of such falsifiable features does not confirm genuineness. (1.) In other words, ‘FIRST LINE INSPECTION’ technologies should have a ‘call to action’ sensory that would psychologically encourage the human senses to easily perform an inspection evaluation to a successful end result i.e.: verify genuineness or falseness.

The importance of the ergonomics of security features to create this ‘call to action’ for ‘FIRST LINE INSPECTION’ to confirm, either false or genuine, is of great importance. Security features make the document either falsifiable; that is capable of being proved false, or verifiable; that is capable of being proved genuine. *Verifiers* are based on virtually immutable

technologies that produce unique, easily observable effects that cannot be simply imitated. The obvious of such an effect reliably confirms the genuineness of the product. Consequently, verifiability is to be greatly preferred over proving falsity. (1)

Today, utilizing digital technology with hand held readers; we can combine non-complex FIRST LINE inspection techniques with integrated SECOND LINE machine-readable capabilities to guarantee image authenticity with a high degree of success.

This paper covers combining printed verifiers and falsifiers – ‘NaNOcopy™/LogoDot™, with embedded imperceptible digital data ‘Digital Watermark’ and substrate embedded imperceptible UV codes ‘TechMark™ that together can be deciphered by a handheld reader ‘VeriCam™ to create the optimum – Lock – Hide a Key – Key security system.

2. HISTORY OF ANTI-COPY TECHNOLOGIES

The first anti-copy features were developed in the late 1970’s by the Burrough’s Company in an effort to protect against analog photocopying. Today the advent of improved digital photocopy equipment, particularly high resolution 600 x 600 dpi digital color photocopy equipment, as well as desktop publishing and digital scanning, has provided the unscrupulous with the means for unauthorized duplication of original documents for the purpose of passing them off, with or without alteration, as the original document. The quality of the reproductions obtainable through these means is so good that it is difficult to distinguish original copies from color reproductions. Even if the duplication is not exact, the reproduction often appears authentic in the absence of the original for comparison. This problem is well-known to the issuers of such original documentation, and considerable attention has been given to find improved ways and means to prevent unauthorized duplication of such documents by modern photocopiers or other electronic methods.

Since the first Burrough’s anti-copy patents, many improved techniques have been developed to prevent improper reproduction of original documents. These older techniques were based on the phenomenon that photographic copiers have an element value (sometimes referred to as element frequency) threshold above which the photocopier is unable to distinguish the individual elements of the pattern of halftone printing. In general, a pattern with a low line screen value of large sized elements is more easily reproducible than a pattern with a high line screen value of small sized elements.

In accordance with this older technique, a hidden warning message, such as ‘VOID’ or ‘COPY’, is printed in a halftone within a halftone background on a substrate. The line screen value of the hidden warning message is selected, such that the elements of the hidden warning message are reproduced when photocopied. The line screen value of the background, however, is selected, such that the elements of the background are not reproduced when photocopied. As a result, the hidden warning message will appear on duplicates of the original document made by photocopying. This method is also used by reversing the screen values of the hidden warning message and the background, such that the elements of the hidden warning message are not reproduced and the elements of the background are reproduced when photocopied or scanned.

In addition to selecting differing line screen values for the hidden warning message and the background pattern to allow them to be used to prevent duplication, it is also known to select differing tonal screen values (i.e., the percentage of element size and thus the amount of ink coverage), so that the hidden warning message more easily appears on a reproduction of the original document.

Because of the disparity between the respective line screen values and respective tonal screen values of the hidden warning message and background pattern, a mere combination of these two techniques may not be effective, because the hidden warning message might normally be visible to a casual observer of the original. To minimize the visible appearance of the warning message with this combined technique, the respective tonal screen values are selected so that they are more similar, and/or a camouflage pattern can be printed over, or combined with, the hidden warning message and background to help obscure the hidden warning message from a casual observer of the original document.

Another anti-copy printing technique was developed in the early 90’s and is referred to as screen angle modulation (SAM). With this technique screen dots are replaced by minimal lines, which are printed in an orientation pattern to mis-register with the scanning frequency protocol and thus produce a hidden warning message on a copy. Increasing the disparity between the hidden warning message and the background pattern utilizing the (SAM) technique and camouflaging the warning message with a thermochromic ink pattern has greatly improved its anti-copy capability.

While the above techniques have provided some degree of protection of original documents with respect to most copiers, in recent years digital scanners and color copiers have improved both their resolution and digital filtering capabilities substantially. These new color copiers, such as the Canon 6LC1120 series can reproduce at a very high resolution of 600 x 1200 dpi and have made the above techniques less effective in protecting original documents. By manipulating the control and filtering settings on such devices, copies can be made of such original documents in which the hidden warning message does

not readily appear on reproductions when some of the older most commonly used anti-copy frequency and element size printed combinations are used. When the contrast/dark-light settings of these modern digital photocopiers is set to the different settings or the copier is set to a built-in filter halftone setting, the resolution of the copiers is such that it reproduces both the lower line screen value and high tonal screen value equally. In most cases, the hidden warning message does not readily appear on the reproduction of the original document, so that a casual observer of the document may not be alerted that the document in possession is not the original.

A greater element disparity between the respective line screen values and tonal screen values of the hidden warning message and background pattern would allow the hidden warning message to appear on a reproduction of the original document even with the manipulation of the copier. Due to this disparity, however, most presently known camouflage techniques do not adequately suppress the visual appearance of the hidden warning message on the original document being rejected as a copy, which would not be acceptable to issuers of the original.

3. EMBODIMENT OF NaNOcopy™ Patent Pending

In accordance with a first aspect of the NaNOcopy™ technology, a document comprises a nano-pattern printed on a paper substrate, wherein the nano-pattern is configured for forming a latent message (e.g., a warning or alert message), which will appear on a copy of the document. For example, the nano-pattern can form either the foreground or the background of the latent message, and be configured, such that the foreground or background exhibits a first visual density on the original document, and a second visual density greater than the first visual density on the copied document (Figure 1).

In the preferred embodiment, the nano-pattern forms a foreground and a background of the latent warning message; and another pattern, e.g., a conventional halftone or screened pattern forms the background around the latent message. The nano-pattern and the other pattern are configured, such that the foreground and background exhibit substantially similar visual densities on an original of the document, and exhibit substantially different visual densities on the copied document. This can be accomplished by forming nano-structures with a plurality of adjacent elements that are configured to create digital frequency disturbances and trap printing matter, such as ink or toner, when electronically copied, thereby darkening the nano-pattern on the copied document. Creating digital copying frequency disturbances and trapping of the printing matter is facilitated by the structure design, modulation and miniature size of the adjacent elements, which are preferably less than two-point print, and most preferably, one point print or less. The modulation and plurality of adjacent elements that make up the nano-pattern can be combined into a series of nano-structures or shapes, e.g., stars, polygons, circles, ovals, crosses, X's, or alpha-numerical characters, to produce the desired darkening effect. The series of nano-structures can either be uniformly sized and spaced, resulting in a regular nano-pattern, or variably sized and spaced, resulting in an irregular nano-pattern. Additionally, the variably sized and spaced nano-structures can be configured in a modulation pattern to form the variably sized and spaced nano-pattern.

In the preferred embodiment, visual density similarity between the nano-pattern and conventional pattern on the original document is affected by printing both patterns using dots, lines, or other suitable element markings. The line resolution value (i.e., numbers of line per inch), tonal screen value (i.e., percentage of ink coverage), modulation frequency, and element size used to form the nano-pattern structure configuration and conventional patterns are adjusted, such that the respective patterns exhibit substantially similar visual densities on the original document. For example, the line resolution value, element size, and tonal screen values for each of the nano-pattern and conventional pattern can be printed to exhibit a visual 10% density value.

The visual density disparity between the nano-pattern and conventional pattern exhibited on a copied document is affected by the darkening or lightening of the nano-pattern when copied. Specifically, the use of the nano-pattern in a foreground takes advantage of the fundamental limitations of optical scanning digital systems and toner or ink jet output devices, which cannot reproduce very minute, fine detailed nano-printing of certain rectilinear or curvilinear nano-structure frequencies. Some nano-patterns are designed, such that ink or toner traps are formed within a reproduction of the nano-pattern. These ink or toner traps fill and darken when electronically ink jet or toner printed. As a result, the ink or toner traps cause the nano-pattern to exhibit an increased visual density when the original document is electronically copied.

Although the visual density of the nano-pattern increases on the copied document, the conventional pattern, on the other hand, is normally reproduced. That is, the conventional pattern is designed, such that there is no frequency disturbances and ink or toner traps are not formed within the conventional pattern. In this respect, the conventional pattern is similar to typical patterns that are printed on original documents. As a result, the visual density of the conventional pattern does not substantially increase and preferably decreases on the copied document. The disparate visual densities exhibited by the respective nano-pattern and conventional pattern, when electronically copied; cause the latent warning message to visually appear on the copied document.

For the purposes of this specification, a nano-pattern and conventional pattern, and thus, a foreground and background, exhibit substantially similar visual densities if a casual observer cannot readily recognize the latent message, and exhibit substantially different visual densities if the same casual observer can readily recognize a latent message.

When two different nano-patterns are used to create a latent message, the visual density similarity between the respective first and second nano-patterns exhibited on the original document is affected by printing both patterns using dots, lines, or other suitable element structures, and accordingly adjusting their element size, line resolution, modulation frequency, and tonal screen values. Visual density disparity between the respective first and second nano-patterns exhibited on the copied document is affected by the darkening of the first and second nano-patterns. The frequency disturbance and ink or toner traps formed in the first nano-pattern, however, are more pronounced than those formed in the second nano-pattern. Preferably, the second nano-patterns are created using structures that copy at the copier's base frequency and does not form any ink or toner traps. As a result, the first nano-pattern exhibits an increased visual density with respect to the second nano-pattern, when the original document is electronically copied.

It is anticipated that further levels of security can be provided by a nano-pattern besides the formation of the latent warning message when copied. For example, using alpha-numerical characters in a nano-pattern has the added advantage of conveying visual or digitally coded electronic reader information to the observer of the original document. That is, the printer of the original document can nano-print a latent message in the form of numbers, words or structures, in effect, embodying a separate message, such as the indicia indicting validity, date printed, customer's name, and /or secret numerical code, within the latent message.

A simple example might be that an observer in possession of the original document, knowing that the original document comprises the repeating words 'VALID' in nano-printing, can review the original document with a magnification aid, such as a magnification loupe. If the repeating word 'VALID' appears in the nano-pattern on the original document, its authenticity is ensured. In contrast, if the repeating word 'VALID' has been obliterated, which will typically occur during the electronic copying process, an observer in possession of the copied document will know it is not authentic.

Additionally, as an example, a nano-number '245032484843' may be used and represent a secret code known only by an authorized person. For example, the number may be an algorism, the nano-digits of which add up to '47'. Optionally, certain portions of the latent warning message e.g., the letters 'I' and 'D' of VOID, may contain nano-numbers that represent meaningless data to further confound the unscrupulous copyist. Furthermore, one or more of the nano-digits in any one of the letters composed in a latent message, i.e., 'V', 'O', 'I', or 'D', can be minutely deviated, such that an authorized person, knowing that a deviated nano-digit exists, and knowing the location, design, and extent of the deviation, can authenticate the original document. In contrast, an unscrupulous copyist would not notice the minutely deviated nano-digit within the generally uniform pattern of all the other nano-digits, making it difficult to exactly reproduce the deviated nano-digit by traditional printing methods. For example, a nano-digit '3' in the right upper hand corner of the 'V' can be printed in a slightly different font than the other nano-digits. Without knowledge of this minutely deviated nano-digit, one would not recognize it within the context of the uniform styled digits. Such minute deviations may not be limited to nano-digits or font changes, but can be incorporated with any nano-structure using any deviation that could be noticed by a knowing individual, but would not be noticed by an unsuspecting individual.

The algorism need not be based on an 'add' function, but may be based on other encrypted functions, the application of which to the number formulation combined with alpha or other structures produces a known answer. Thus, an authorized person in possession of the original document knowing the specific encryption formulation of the repeating nano-structures that appear in the nano-pattern on the original document can review the original document with the magnification aid. If the repeating nano-structures are confirmed, its authenticity is ensured. In contrast, if the repeating nano-number has been obliterated, which will typically occur during the electronic copying process, an observer in possession of the copied document will easily know that it is not authentic.

Furthermore, the encrypted nano-pattern has the potential to carry machine-readable data for full spectral analysis of the optical characteristics of the nano pattern's microstructures. This data can be evaluated by performing an optical correlation of the reflection spectrum of the document to be validated with the original document. One such device is Appleton Security Product's VeriCam™ hand held reader. Thus, other much higher levels of security are provided on top of that provided by the appearance of the latent message, itself (Figure 2).

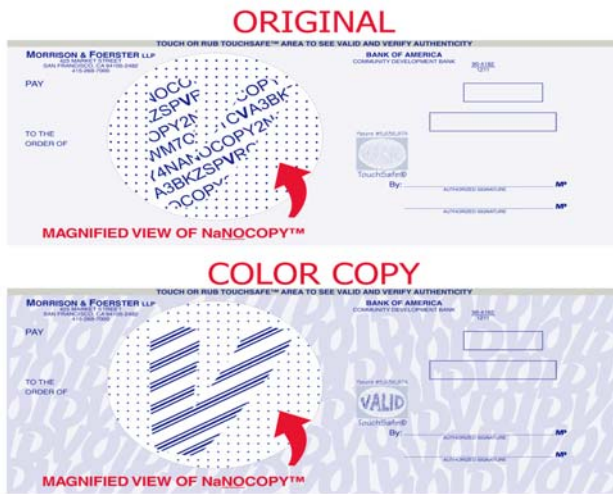


Figure 1. NaNOcopy™



Figure 2. VeriCam™

4. Embodiment of LogoDot™ patent pending

The LogoDot™ technology is similar to the NaNOcopy™ technology except it utilizes a digital conversion process to capture and micro size any graphic for halftone-vignette printing.

The building-block of digital imaging is the pixel. Pixels are those tiny points of light that you see on your computer display when you examine it with a magnifying glass. On color displays, carefully focused pixels are arranged in red, green, and blue clusters to simulate various hues that are modulated in brightness to approximate color intensities. Laser printers apply a charge to a magnetic recording surface with a sweeping beam that flashes at the center points of pixels. Scanning machines reverse the action of the pixel to ‘read’ an image through a moving array of sensors. Pixels are the smallest addressable element under the control of the device. The spacing of these pixels is referred to as the resolution of the display, scanner or printer.

Within the printing industry, device pixels are truly microscopic. Image-setting machines we use to make printing plates employ pixels that are approximately 1/2500 of an inch (or smaller) in size. Compared to a standard computer display, these machines have as much as 30 times more pixel resolution. Although computer displays cannot accommodate images at these resolutions, regular printing plates and paper handle them well. Hundreds of pixels are typically illuminated together to create a halftone dot. For instance, a single halftone dot used in standard 133-line commercial printing is constructed from 366 (or more) individual pixels. Based on the virtues of offset halftone printing, a new technique has been developed that exploits paper’s exceptional resolution-holding potential. Amgraf, Inc., a company located in Kansas City, Missouri, has developed LogoDot™, whereby the halftone dot itself is being commercialized and used to store microscopic images. And once printed on paper, these images cannot be accurately copied.

Using LogoDot™/DotMaker™ software, one can image a corporate logo, a photograph, or a key word or phrase, and convert that image into a custom halftone screen dot. One can control the ‘growth’ of the ‘logodot’ (containing the microscopic image) with tonal variation features so that it can successfully be used from very light to very dark area of the printed document or object (Figure 3).

The LogoDot™ method also has applicability in the manufacture of secure documents, labels, decals, tags, identification cards, packages, and other printed products. In addition, the LogoDot™ method has value for artistic design beyond the utility of security document protection. The ability to include one’s corporate logo or self-portrait as a microscopic image within a printed document or object has the appeal of added personalization or validation. As an example, Verify First Technologies has developed a security envelope that utilizes LogoDot™ printing on the inside of the envelope, which can be verified through a unique window to help enforce recipient confidence that the mail piece has originated from a trusted source. Additionally, the ability to name and recall the ‘logodots’ is the foundation for building libraries of custom dot designs for various commercial, industrial, and artistic purposes.

The LogoDot™ technology utilizes a DotMaker™ software program that takes a rectangular, digital bitmap as a ‘seed image’, and converts it to a printing spot. The seed image is placed in a square cell, whose side length (in terms of number of pixels) is the larger of the 2 sides of the image. For practical purposes, the current implementation limits the seed image to be no more than 255 pixels on either side. While increasing the number of pixels has the benefit of adding detail to the microscopic image, a lower line frequency must be specified in order for every pixel within the custom dot to be displayed.

Any size pixel matrix can be used from 2 x 2 to 255 x 255. For screen frequencies other than the ideal, PostScript automatically inserts or removes pixels from within the custom halftone cell to output the specified lineage. If the image is gray-scale, each pixel’s darkness value is used as the ‘pixel ranking values’ for the spot cell, where black corresponds to the highest ranking value, and white the lowest. These ranking values therefore reside inside the limit between zero and the highest value that each pixel size in the image can accommodate. For images stored with one byte per pixel, the limit is 255. (c.) If the image is color, it is converted to gray-scale by using the commonly known Red Green Blue (RGB) color to Luminance calculation.

The DotMaker™ program allows the user to save and refer to custom dots by name and assign screening attributes to any graphical element in a document layout. Custom dot designs are given a unique name and collected in a Custom Dot Library, which can be utilized, by the MECCA 2000 Integrated Electronic Publishing Systems manufactured by Amgraf, Inc.

The procedure to follow in order to create a security document that contains the custom LogoDots™ is as follows: (a.) The designer captures a ‘seed’ image to use as the ‘logodot’. The image can be scanned from a hard copy of the image or obtained via a digital camera or other means. The image then is reduced to a rectangular ‘bit-map’ with an overall pixel count not to exceed 255 x 255 pixels (b.) Using standard desktop publishing pixel editing software, the bit-map is edited to indicate the preference for progressive illumination of the pixels from white to black, by making the most prominent pixels black, the least prominent pixels white, and the order of tonal variation across the dark to light spectrum in various shades of gray. (c.) The resultant ‘seed’ image is saved from the pixel editor program then loaded into the ‘DotMaker’ program, named, and processed into a ‘logodot’ consisting of illumination ranking instructions. (d.) The code set is stored in a Custom Dot Library on a MECCA 2000 System. (e.) A MECCA 2000 user creates or opens a design file for a security document and assigns various custom dot names (and screening attributes) to various graphical elements such as photographs, text and typefaces, rules and lines, circles, arcs, splines, colored areas, borders, pantographs, patterns, and logos. (f.) The MECCA 2000 user selects the ‘Output’ menu and sends the composite image to a PostScript imaging device to create printing plates, negatives, and/or films which contain the ‘logodot’. (2)

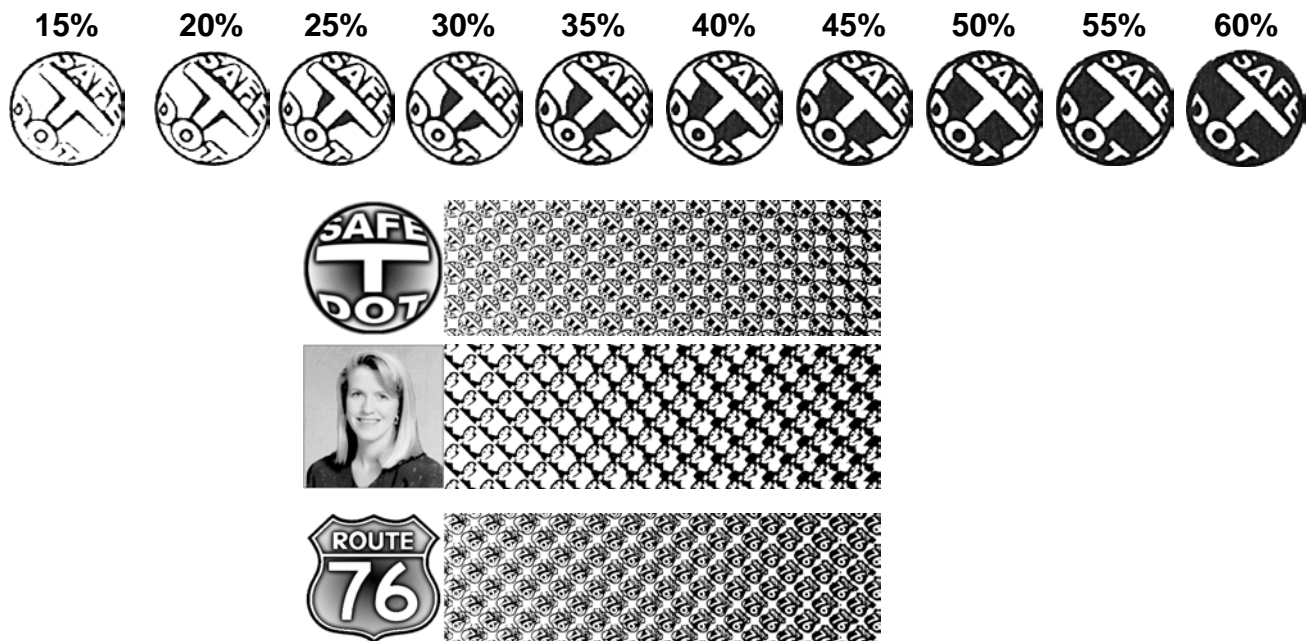


Figure 3. LogoDot™ Preview of the dot images with density progression.

As with the NaNOcopy™, the LogoDot™ has the potential to carry machine-readable data for full spectral analysis of the optical characteristics of the LogoDot™ nano pattern’s microstructures.

5. EMBODIMENT OF TECHMARK™

Spectra Systems Corporation, in collaboration with Appleton Security Products, has developed machine-readable encoded taggents embedded in a security paper substrate. Appleton has trademarked their machine-readable papers, TechMark™ ‘intelligent’ solutions.

The embedded taggent particles are invisible under ordinary light, but are brightly fluorescent under UV light, which allows for quick visual checks for authenticity. These rare multi-colored UV particles are embedded into the paper substrate at the paper making process and are formulated to create unique signature codes, which can be identified by a hand held ‘VeriCam™’ reader (Figure 4). The rare impregnated UV particles come in two sizes with six color variations to create over 200 unique machine-readable batch code signatures. The VeriCam™ hand held reader offers a broad range of features including the capturing and storing of images in its picture photo mode. It also functions as an integrated management terminal for route management and production control to protect against product diversions. Additionally, the VeriCam™ will identify encrypted imperceptible digital pixel modulation; i.e. digital watermark.



Figure 4. TechMark™ UV Taggents



Figure 5. VeriCam™

The real power of the TechMark™/VeriCam™ combination is that the unique UV taggent code signature can be used as an opener to a secure gateway that would allow the reader to identify the other mentioned technologies; e.g., NaNOcopy™ - LogoDot™ - Digital Watermark. Unless the reader detects the correct UV code taggent, access to the second or third technologies is denied.

An example of how a perfect secure scenario might be; a secure document would be printed on Appleton’s TechMark™ ‘intelligent’ paper, which is impregnated with a specific UV taggent code. The secure printing would incorporate a NaNOcopy™ background and a specific LogoDot™ area, which would also include a digital watermark. The VeriCam™ reader would first read the unique UV taggent, which would act as a ‘Hide a Key’, or first stage, to open the reader. The reader would then open up a gateway and allow the magnified viewing of the secure NaNOcopy™/LogoDot™ printing and verify authenticity by a known algorithm or deviation of the nano structures. The reader and the human viewer would act as a ‘key’, recognize the known attributes, and allow entry to the third aspect of the layered security system. The third and final check would be considered the opening of the ‘LOCK’ that allows the viewer an absolute guarantee of authenticity. The viewer would reference a specific LogoDot™ area, which has an embedded digital watermark and since the first stage ‘Hide a Key’ UV taggent code has already activated or unlocked the decoding for the digital watermark the VeriCam™ confirms the final stage of absolute authenticity (Figure 5).

- 1 – UV Code = Hide a Key
2. – NaNOcopy™/LogoDot™ = Key
3. – Digital Watermark = Lock Opening

6. CONCLUSION

In this paper we introduced the concept of utilizing minute nano structures - NaNOcopy™ and LogoDot™ - for digital anti-copy purposes and combining these technologies with imperceptible substrate UV code - TechMark™ - and imperceptible digital information - Digital Watermark - to create optimum machine-readable security.

Any one of these technologies, when used independent of each other, can supply a very high level of security. However, when used together with a hand held reader, which ties them to confirm genuineness, one can guarantee image authenticity with a probability approaching certainty. Full utilization of combining and tying the technologies is dependant on software development of sophisticated machine readers, some of which are currently under development. One such reader, 'VeriCam™', mentioned in this paper, presently has the capability to read and combine these technologies to confirm authenticity.

It is reasonable to expect further migration to develop more sophisticated combinations or layers of protection of binary printing technologies combined with unique hand held readers.

REFERENCES

1. R.L. van Renesse, "*The Human Factor of Security*", TNO Institute of Applied Physics, Document Counterfeiting Protection, Paper 14, 1999
2. Franklin J. Garner, III., "*New Security Technologies for Printed Documents*", Business Printing Technologies Report, October 2001 - Amgraf, Inc. www.amgraf.com
3. Amgraf, Inc. is the developer of MECCA™ Integrated Electronic Publishing System and LogoDot™/DotMaker™ Software
4. Appleton Security Products is a security solution provider, which provides security papers and anti-fraud solutions. TechMark™ is an Appleton trademark. www.appletonpapers.com
5. Spectra Systems Corporation is the developer of the unique TechMark™ taggents and VeriCam™ reader. www.spsy.com

*Contact: Author, George K. Phillips, Verify First Technologies, P.O. Box 7001, Paso Robles, California 93447 USA
805 238 2503 fax 805 238 7213 email: george@verifyfirst.com www.verifyfirst.com