A Multi-Spectral Approach to covert data

D. Padiyar, J. Padiyar, R. Billmers

Abstract

Covert information applied to holograms is based on size, geometry and physical structure. The encoded information is either extremely tiny/machine readable, based on various assorted different geometrical patterns or is embedded in a physical structure by which any tampering of the product damages part of the product in an obvious and easily discernible way. However, each of these techniques relies on a multiple of single events, each of which are tested individually and sequentially. Therefore to confirm that each of these security devices have not been compromised requires a multitude of individual tests. A parallel solution to the security question is proposed whereby several tests are carried out simultaneously. In this manner, only one test is carried out and any failure mode in any one of the security devices is detected at once. Thus, it is proposed that N gratings at N different wavelengths are recorded and are read out by some pieces of equipment simultaneously. The outputs of the readout are passed through an AND gate, or some form of optical AND gate, so that a single test will simultaneously probe a multi-spectral signature and a failure for any given wavelength will result in a "no-go" state.

Introduction

The use of holograms as a security device is now roughly 30 years old, starting from the early 80's with the Visa dove. The security aspect relied on the fact that the hologram required skills that were not possessed by many, such skills being difficult to acquire and expensive to implement. In addition, the necessary equipment for mass production of these holograms are/were expensive and not easy to obtain. Over the years, these limitations have been overcome, so that the methods of making a hologram are easily available on the internet, the equipment is now relatively cheap and there exists a size-able community from whom information concerning previously specialised techniques can be easily obtained. As a result, the security aspects of holograms have become more and more sophisticated.

We would like to divide the methods of security in holograms into three broad categories:

1. Overt security

2. Covert Security

3. Overt/Covert Security

Overt Security

This kind of security relies on the fact that a hologram exists and is freely visible. The advantage of this feature relies on the fact that the hologram is instantly visible and recognisable. The unique look of a hologram is easily discerned and difficult to emulate by non-holographic means. However, this kind of security can be easily compromised by a hologram of inferior quality, since the public at large tends not to notice differences between the quality of a genuine hologram and a badly copied version. In addition, the genuine hologram can be contact copied to reconstruct the hologram. The contact copying technique is relatively easy to implement but it has it's drawbacks, depending on the nature and complexity of the hologram. The copy hologram will be of a lower quality than the original, but will pass a casual inspection.

Covert Security

This kind of security rests on features embedded or recorded within the hologram. These features are not clearly visible, but can be revealed by use of commonly available equipment. The security aspect of these techniques relies on the ignorance of their presence within the hologram. However, these features are easily discerned if knowledge of these features could be obtained. Some examples of these include:

a)Hidden imagery, in which a hologram of some shape or some text is recorded holographically within the hologram. The imagery is designed to be viewed by a laser beam at some specific angle and is projected to some particular distance. A diffusion screen placed at the correct distance and angular position will reveal the text or shape. This method relies on ignorance of the correct angle with which to illuminate the hologram, but detailed inspection with a laser beam will reveal the feature

b) Micro-structures, in which micro-text or specific micro-figures can be imprinted onto the hologram photographically. Thus the words "Security Feature" can be photographically encoded at a feature size of a few microns. If the feature size of the order of 10s of microns, it is visible with a magnifier of 10X or greater such as a loop, if this feature is known to be present. If the feature size is smaller, as may be recorded with an electron beam, the feature will diffract when illuminated with a laser at the correct angle. Once the position and content of such microstructures is known, copying them is not difficult.

c) Geometric variations, such as altering the geometry of a dot in a dot matrix machine. Thus, the dots of a dot matrix machine may be hexagons or triangles. These variations may exist within a hologram, so that at specific positions within the hologram some dots are of a different geometry from other dots. This feature is visible with a microscope and so the feature may be discovered, but it is not easy to copy.

c)Luminescent overlays, such as dyes, may cause a feature to glow under a UV lamp. These are common dyes and are available.

Covert/Overt Security

In this section we refer to the feature in a hologram that exists in the structure of the material in which the hologram is embedded, that is, the substrate of the hologram. Thus the hologram is clearly visible as an overt feature in the sense noted above, but has a covert feature not visible until the hologram is tampered with, at which point the tampering is evident. We feel that this is not so much a security feature per se, but a method for ensuring the product itself has not been compromised.

A Multi-Spectral Approach

The essence of any security feature are:

1. The difficulty in reproducing or reconstructing the security feature by an unauthorised user, i.e. the complexity of the security feature

2. The simplicity in decoding the security feature by a genuine user, in that a dedicated, easy to use machine give an instant go/no-go condition.

3. The cost and ease of implementation of the security feature. The feature must be encoded at a low cost with existing equipment which can easily be manipulated to create the security feature.

The methods in use at present satisfy these criteria independently with varying degrees of success. However, the implementation of some of these features may be mutually exclusive. Thus, the greater the difficulty of reproducing or reconstructing the security feature, the more complex may be the implementation of the feature. In such a case, while criterion 1 is satisfied, criterion 3 is not.

The Proposal

We propose a multi-spectral approach to security that satisfies all three criteria noted above. It would be fairly difficult for an unauthorised user to reproduce, it can be decoded in a simple way and could be implemented by equipment already in existence in production houses by personnel with present levels of training.

We propose that we record specific spatial frequencies in the hologram, such that specific narrow band sources, placed at specific positions diffract to specific detectors placed at particular positions. These detectors are designed such that they will only accept light in a narrow band of wavelengths, tuned to their appropriate illumination sources. Thus, leds at lambda1, lambda2…lambda n are placed in certain positions p1, p2..pn vis a vis the hologram. These leds hit the hologram at specific angles such that they diffract to detector 1, detector 2…detector n. All the detectors have narrow band filters in front of them, so that only light from their corresponding led will be registered. Any light to the detector from a non-corresponding led will not register because the filter in front of the detector will not allow the light to enter the detector. The output from various detectors are combined into an AND gate, which will emit a signal only if the output from all the detectors simultaneously register. If any one of the detectors does not register a signal, the AND gate will not emit a signal. The presence of a signal from the AND gate will be recognised as a "go" condition, perhaps by turning on a green light, while the lack of a signal from the AND gate will enable a red light signaling a "no-go" condition.

In this representation, only a specific wavelength range impinging onto the hologram at the correct angle will diffract to the correct detector. Any other direction of the band of wavelengths will not diffract to it's corresponding detector. Similarly, any other wavelength at the correct angle for different wavelength will not be detected by the detector since the detector has a filter in front of it to block all but the correct wavelength range. Hence, only the red led at the correct red position will diffract red light to the red detector and send the correct signal to the AND gate. Any other colour of led, besides red, at the red led position will not diffract to the red detector. Any other led diffracting to the red detector will not be detected.

Variations

There are variations on the above representation that may enhance the security aspects of the method. The leds may be arranged in any given geometry, such as in a circular pattern. In

addition, the detectors may also be placed in a different pattern, such as arranged as the sides of a square. The specific pairing of any given led to any given detector is also user defined. This gives a very large number of permutations of possible source/detector combinations. The larger the number of source/detector combinations, the greater are the number of possible permutations. In addition, it would be relatively simple and quick to alter the source/detector combinations at regular intervals. Thus, an led may diffract to it's corresponding detector at some position p1, but it is possible to have the same led diffract to a different position p2 very easily.

Implementation

This method is fairly simply implemented by determining the source/detector combination. The appropriate spatial frequency necessary to diffract the given led source to its corresponding detector can be easily calculated. This spatial frequency may then be recorded by determining the positions of point sources needed for the laser under use; mirrors placed in such positions will record the appropriate spatial frequencies. Thus, for example, it may be determined that a red led from a pre-determined position will diffract to a red detector at another pre-determined source. The appropriate spatial frequency is calculated. Then the angles of beams necessary to record this spatial frequency at the recording wavelength of, e.g., 457nm is calculated and mirrors are placed to create beams at this angle. The "red" spatial frequency is thus recorded with the standard blue laser.

If the source/detector positions are known, then a detection device may be built into which leds and detectors, appropriately filtered to only receive the wavelength range they're designed for, are attached. The output of all the detectors are detected optically, converted to an electronic signal and sent electronically to a gate. If all the detectors register an "OK" signal, the gate will signal a "go" condition. However, if any one of the detectors does not register, then that particular detector will emit a "not OK" signal and the gate will emit a "no go" condition. Thus, simply inserting the hologram into such a device will enable either a green "go" condition, or a red "no go" condition.

Advantages

The multi-spectral wavelength approach confers a number of advantages. The number of possibilities of source/detector combinations goes up factorially as the number of source/detector combinations. Thus, for 5 source/detector combinations, there are factorial 5,

or 5x4x3x2 = 120 different possible combinations. Typical filters allow have a bandwidth of roughly 50 nm, so that the entire visible range of 400nm can be covered with 8 leds, giving 8x7x6x5x4x3x2 = 40320 possible combinations. Narrower filters may be obtained for a greater number of combinations. The exact combination may be easily switched for a next generation or new security feature, or simply for a new run of the same product. Thus, the red led may go to a position p1 in one situation, but may be switched to position p2 in another run of the same product. This simply involves calculating a new spatial frequency and placing the mirrors accordingly. In addition, the source geometry and the detector geometry are unrelated and so may be changed. Thus, the sources may all be placed in a circular pattern with the detectors on the sides of a square for one particular run, then switched for the next run.

Random illumination of the hologram with a laser will not reveal the specific source detector combinations, since it would be necessary to illuminate the hologram with wavelengths of all the leds simultaneously at the correct angle. It may be possible to examine the detection device and so determine the spatial frequencies necessary to give a “go” condition and then to construct a similar detection device. However, if and when this has been detected, it is possible to confound this approach by simply switching to a new source/illumination geometry.

Contact copying a hologram with this multi-wavelength set of gratings will not allow the copying of all the source led wavelengths at the correct angles. It may allow the diffracted light from one led to go to a detector, but the light will go to the wrong detector and so will not register. When a hologram is contact copied, the copy beam reconstructs the hologram so that the object of the copy hologram is the reconstructed object from the master hologram and the reference of copy hologram is the copy beam. In the multi-spectral system presented here, any single copy beam will reconstruct beams from all the multi-spectral spatial frequency components and interfere them with the single copy beam. This will give rise to a set of new spatial frequency components that are not the same as the original multi-spectral spatial frequency components. This will result in the led sources diffracting light to the wrong detectors and there, as mentioned earlier, will result in a “no-go” condition.

Conclusion

We believe we have developed a method of recording a security feature on holograms that is simple and cheap to implement, simple to use in the detection of fraudulent product, highly flexible so that the security aspect can be easily altered.