Secure Information Hiding based on Computationally Intractable Problems

S. Armeni[1] D. Christodoulakis[1,2] I. Kostopoulos[1,2] Y.C. Stamatiou[1,2] M. Xenos[1,2,3]

[1] University of Patras, Department of Computer Engineering and Informatics, Rio 26500, Patras, Greece.
[2] Computer Technology Institute, 61 Riga Ferraiou Str., GR-261 10 Patras, Greece.
[3] Hellenic Open University, Sachtouri 16, 262 23, Patras, Greece.

Abstract. [1]
In this work, a method for proving copyright ownership is presented that is based on Zero Knowledge Interactive Proof (ZKIP) protocols for computationally intractable problems. The utilized problem is the *3-coloring problem*, which consists in assigning one of three available colors to the vertices of a graph so that no two *adjacent* vertices have the same color. Using the presumed computational intractability of this problem, the construction of large signatures is proposed so that they represent adjacency matrices of random, 3-colorable graphs. Since it is *easy* to construct large graphs with a prescribed 3-coloring of their vertices whereas it is difficult to *discover* such a 3-coloring, the owner of a copyrighted digital piece of work (e.g. image, audio, video) may easily generate a random 3-colorable graph, embed it in the digital object and then use the knowledge of the 3-coloring in debates over the object's ownership. Due to the intractability of the 3-coloring problem, only the owner is able to produce it sufficiently fast in an ownership challenge so as to convince a third party that the graph was indeed embedded in the object by herself/himself. Since graphs with maximum possible resistance to well-known coloring algorithms is required, we exploit some relatively recent experimental and theoretical findings suggesting that hard 3-coloring instances are found among graphs having a vertices to edges ratio around a specific *threshold* value. The proposed scheme has the additional advantage that disclosing the signature is of no consequences since it is essentially the *knowledge* of a characteristic of the signature, i.e. the 3-coloring of the graph it represents, that enables one to use it as proof of ownership of some digital object that contains it. Even if someone managed to locate and extract the signature, to use it would require a fast solution to a computationally intractable problem on some *hard* instance. Our proposal represents a shift from signatures that are simply viewed as bit sequences to signatures with properties that stem from their interpretation as instances of computationally intractable problems.

Keywords: Cryptography, Data hiding, Zero Knowledge Interactive Proof (ZKIP) Protocol, Hard Combinatorial Instances, NP-completeness, 3-coloring, Graph Theory.

[1] This is a pre-print version of the paper published in *Journal of Discrete Mathematical Sciences & Cryptography*, Vol. 6 (1), pp. 21–33, April 2003.

1 Introduction

The appearance of inexpensive data reproduction means as well as the widespread use of Internet, exposes digital material to unauthorized modification, duplication and redistribution more than ever. The necessity of protecting copyrighted digital material such as audio, still images, and video has led to the introduction of a variety of signature-based protection methods (see [3, 11]) that provide solutions to the problem of verifying the owner of the material. Most of the methods embed some user-specific bit-sequence in the material to be protected that, when detected, uniquely identifies the legal owner in cases of copyright related disputes. A disadvantage (see below) of such methods, however, is that one may steal the signature and use it subsequently to impersonate the rightful owner.

In this work, a different approach to this problem is presented based on a Zero Knowledge Interactive Proof (ZKIP) protocol (see Papadimitriou [20] for example) for the computationally intractable *3-coloring problem* (it is NP-complete–see [12]). In this problem the user's signature represents the adjacency matrix of a random 3-colorable graph with edges to vertices ratio within a region that, experimentally, is known to produce instances that are most hard to collor as shown in Section 2. The computational difficulty of producing a 3-coloring for such instances can be considered as a strong evidence in a copyright dispute in favor of the person who can exhibit *fast* a 3-coloring for the graph representing her/his signature.

The method described in the sections to follow, can also be viewed as a proposal for an alternative characterization of a strong signature. The focus is shifted from signatures that possess certain statistical properties (e.g. being random), or signatures representing a company logo, to signatures that when interpreted properly they represent a combinatorial object (graph in our case) with a hard to compute characteristic (3-coloring, for example). Moreover no other person could use another person's signature, even if she/he had managed to extract it from the digital object, which is also a difficult task since it requires knowledge of a, perhaps, complex embedding process. This is due to the difficulty of exhibiting a 3-coloring of a graph which, of course, the legal owner of the object already knows and can readily exhibit. Such a signature, whose usability requires solving a computationally intractable problem, provides an example of a *cryptographically secure signature* in analogy to the *cryptographically secure pseudorandom number generators*.

On another front, there is a vast literature on *threshold phenomena* in intractable combinatorial problems: it has been experimentally observed that for many of these problems there is a value for some critical parameter around which there seem to cluster difficult problem instances (see [6, 14, 17] for good, non-technical expositions to this phenomenon for the *Satisfiability Problem*). Moreover, whenever the value for the critical parameter is slightly below the critical value almost all randomly produced instances do have a property (e.g. 3-colorable graphs) while the opposite holds true for values of the critical parameter slightly above the critical value. For example, in 1991 ([5]) Cheeseman, Kanefsky, and Taylor observed that for randomly produced graphs with edges to vertices ratio at around 2.3, even the best 3-coloring algorithms had more difficulties in coloring the graphs. This offers an interesting possibility for producing random signatures with prescribed hardness.

Variants of the concept of Zero Knowledge authentication have appeared in the past. In [15], Hirotsugu constructs signature graphs whose topology depends on the properties of the image in which they are to be embedded. Then he exploits the computational intractability of the graph isomorphism problem and a ZKIP protocol for it to prove ownership of the image without revealing the signature graph. In [9], Craver uses the computational intractable Hamiltonian Path problem in order to produce a difficult to discover scrambling of the data to be protected. Then he gives a protocol that proves ownership of the data without revealing the signature string. Our approach is in sharp distinction with both approaches in that our signature string *may be revealed* with no consequences since its usefulness lies in the knowledge of a three coloring of it when interpreted as a graph. The proposed Zero Knowledge variation applies on a second level, on proving knowledge of a “meta-property” (3-coloring) of a bit-string (signature). Revealing the signatures' position in the pretected data is of no harm since in order to be utilized by someone else, she/he would have to discover a 3-coloring, which is difficult computationally. Our approach also differs from Hirogutsu's on another respect. Our signature string *does not* depend on the data to be protected. This gives us freedom in the construction of the signature so that it is of adequate hardness, using the theory of threshold phenomena of hard combinatorial problems.

The paper is organized as follows: In Section 2 a method for producing random 3-colorable graphs is described, along with a 3-coloring of its vertices. In Section 3, a well-known Zero Knowledge Interactive Proof (ZKIP) protocol is given for proving knowledge of the 3-coloring without revealing it, while Section 4 describes a signature system based on the computational intractability of 3-coloring and the ZKIP protocol. In Section 5, as an application of the proposed general signature scheme, a method is proposed for proving ownership of digital images. Finally, in Section 6 there is a discussion of the focal issues of the paper as well as some thoughts for future investigations.

2 Producing Random Hard Instances of the 3-Coloring Problem

A graph $G = (V, E)$, where V is the set of vertices and E is the set of edges of G, is 3-colorable if its vertices can be colored using at most three colors so that no two adjacent vertices are assigned the same color. A color assignment that respects this constraint is called a 3-coloring of G.

While it is difficult to color a given graph using three colors, as this problem is *computationally intractable* or *NP-complete* (see Papadimitriou [20] and Garey and Johnson [12]), it is nevertheless easy to *construct* a 3-colorable graph randomly along with a 3-coloring of its vertices. An algorithm that achieves this is the following:

1. Let p_1, p_2, and p_3 be real numbers such that $p_1 + p_2 + p_3 = 1$ and $p_1 p_2 p_3 \neq 0$.
2. Generate a random permutation $i_1, i_2, \ldots, i_n$ of the numbers $1, 2, \ldots, n$.
3. For each $j = 1, \ldots n$, vertex v_j is assigned to color class C_k with probability p_k, $k = 1, 2, 3$.
4. For each pair u, v of vertices that do not belong to the same color class, introduce the undirected edge (u, v) with probability p.

For *any* value of p, the above algorithm is guaranteed to produce a *solved* instance of the 3-coloring problem with color class sizes (expected) $|C_1| = p_1 n$, $|C_2| = p_2 n$ and $|C_3| = p_3 n$. The algorithm provides both a 3-colorable graph along with a coloring of its vertices. However this does not suffice. What is actually needed, is a 3-colorable graph for which it is also hard to find a 3-coloring. In other words, a hard instance of the 3-coloring problem is sought. An interesting possibility for creating such instances comes from the area of threshold phenomena in combinatorial problems.

Let G be a random graph with m edges and n vertices and r the ratio m/n. In 1991, Cheeseman, Kanefsky, and Taylor (see [5]) demonstrated experimentally that for values of r that cluster around the value 2.3, randomly generated graphs with rn edges were either almost all 3-colorable or almost none 3-colorable depending on whether $r < 2.3$ or $r > 2.3$ respectively. This suggested that there is some value r_0 for r around which an abrupt transition can be observed from almost certain 3-colorability to almost certain non 3-colorability of the random graphs. From a complexity-theoretic perspective, however, their crucial observation was that graphs with edges to vertices ratio around r_0 caused the greatest difficulty to the most efficient graph coloring algorithms.

To return to the algorithm that produces solved instances of 3-colorability, it seems that a reasonable selection for the edge probability p would be one for which the *expected* ratio $\mathbf{E}[r|$ is equal to $\mathbf{E}[m]/n$ is around r_0. Thus p is obtained from the following, assuming that $|C_k| = p_i n$, $k = 1, 2, 3$ (i.e. they contain exactly the expected number of vertices):

$$r_0 = \mathbf{E}[r] = \frac{\mathbf{E}[m]}{n} = p(p_1 p_2 + p_1 p_3 + p_2 p_3)n.$$

Thus, one can set $p \sim \frac{r_0}{(p_1 p_2 + p_1 p_3 + p_2 p_3)n}$. It has also been experimentally observed that instances are more difficult to solve when all color classes are of about equal size so setting $p_1 = p_2 = p_3 = 1/3$ resutls to $p \sim 3r_0/n$.

In this way, one samples from the "hard-instance" region of the variables to ratio spectrum of the random graphs. What is not, however, clear is whether this sampling is biased towards instances that may contain many colorings besides our own. This may have the undesirable effect of an opponent stealing our graph and discovering one of these colorings, thus using our graph as her/his own signature. A similar concern about the satisfiability problem with clauses of 3 literals (3-SAT) is expressed in [1]. The problem considered there is the generation of random formulas with clauses to variables ratio around the threshold value that are, however, constructed so as to satisfy a given truth assignment (similar to the construction of a 3-colorable graph). The problem is that the obvious methods to achieve this seem to produce formulas that, apart from the desired assignment, also satisfy many more assignments. This again might have the averse, for our aims, effect that when such formulas are given as inputs to randomized algorithms such as *Walksat*, they may be easier to solve than the satisfiable formulas that are sieved out of the formulas produced uniformly around the threshold value by a 3-SAT formula generator. The area of hard *solved* instance generation is a very active one and there is much ongoing research aimed at building instances with a *limited* number of solutions.

3 A Zero Knowledge Interactive Protocol for 3-Coloring

For completeness of the presentation, this section describes a well known Zero Knowledge Interactive Proof (ZKIP) protocol of one's knowledge of a 3-coloring of a 3-colorable graph. A ZKIP has the desirable property that one may provide convincing evidence of her/his knowledge of a property of some object (e.g. a 3-coloring of a graph) without revealing any information about it.

Let A be the person who knows a 3-coloring of the vertices of a graph $G = (V, E)$ and B the person who wants to be convinced of A's knowledge of the coloring. Let also 00, 11, and 01 be a bit representation of the three colors. For some vertex $v \in V$, its color will be denoted by $C(v) = b_1 b_0$, where b_1, b_0 are each 0 or 1.

The ZKIP protocol is comprised of a number of rounds. At each round, the following steps are executed (see, for example, [20]):

1. A produces a random permutation of the three colors. Thus, the color of each vertex is changed according to the permutation.
2. Then A generates $|V|$ RSA cryptosystems, one for each vertex v. The i-th cryptosystem, for vertex v_i, consists of the elements (p_i, q_i, d_i, e_i) where p_i, q_i are two large prime numbers (one can easily generate large, random prime numbers using a fast, probabilistic, primality checking algorithm like the Miller-Rabin test), d_i is the private decryption key and e_i is the publicly available encryption key (they can be easily produced using Euclid's algorithm for finding the largest common divisor of two numbers).
3. Then for each vertex v_i, A probabilistically encrypts the new color $C'(v_i)$ of v_i. Suppose that $C'(v_i) = b'_1 b'_0$, where b'_1, b'_0 are the two bits representing the new color. Then the following two operations are secretly performed, where $n_i = p_i q_i$ and x_i, x'_i are two randomly generated integers no greater than $n_i/2$ (the operations that follow can be easily performed using the repeated squaring technique):
$$y_i = (2x_i + b_i)^{e_i} \bmod n_i$$
$$y'_i = (2x'_i + b'_i)^{e_i} \bmod n_i.$$
4. Finally, A reveals to B all the (y_i, y'_i, n_i, e_i) for the vertex v_i.
5. B chooses at random an edge connecting vertices two vertices v_i, v_j. Then A reveals the secret keys d_i and d'_i and that were in the RSA system used for the encryption of the colors of the corresponding vertices. B decodes the encrypted color bits as
$$b_i = (y_i^{d_i} \bmod n_i) \bmod 2.$$
and, similarly for b'_i, b_j, b'_j, and checks that the colors are different.
6. The above steps are repeated $k|E|$ times where k represents the *reliability* of the protocol.

Now if A did not really possess a 3-coloring, there would be a non-zero probability that A would get caught at some step. When $k|E|$ *independent* rounds have been executed, this probability is at least
$$1 - \left(1 - \frac{1}{|E|}\right)^{k|E|} \geq 1 - e^{-\frac{1}{|E|}k|E|} = 1 - e^{-k}.$$

The last expression approaches 1 exponentially fast with k, meaning that almost surely A will be caught lying after a number of repetitions of the ZKIP protocol. The important characteristic of the ZKIP protocol above is that not only it provides strong evidence of our knowledge of the coloring but by permuting and encrypting the colors, it effectively erases B's knowledge about the coloring as well. At each round, B is only given the obvious fact: that in a 3-coloring of a graph the vertices of an edge are colored differently (but B cannot tell which are the colors of the vertices). This offers the possibility to A of reusing the signature many times since no information is revealed about it.

4 A Signature System based on the ZKIP for 3-Coloring

The application of the zero-knowledge interactive protocol we presented in Section 3 to signature creation and verification involves three parties:

- The owner of the original digital object (A).
- The person who attempts claim the digital object as her/his own (B).
- The referee (C).

The interactive protocol described below is zero-knowledge, as far as revealing the signature (3-coloring) to the referee is concerned, and provides a proof of ownership of the digital object. The owner, A, embeds in the original object O a sufficiently large 3-colorable graph that was produced using the procedure outlined in Section 2 using techniques described in Section 5. What A actually embeds, is the graph's adjacency matrix which for an undirected graph without loop edges requires $n(n-1)/2-n$ bits. Let O' be the resulting digital object which she/he publishes e.g. on the WEB. Suppose now that B downloads O' and claims ownership. Then A may convince a third party, say C, that A is the owner as follows:

1. A says to C that there is a set of bits in B's object O', that represent the adjacency matrix of a graph of which A knows a 3-coloring.
2. A gives to C the method to extract the *positions* of the bits of the adjacency matrix and A and C start executing the zero knowledge protocol described in Section 3.

Now if B claims that she/he owns the object too, she/he challenged her/him to show her/his signature in O, the *original* digital object which only A may possess since she/he only publishes the marked object O'. Also, O is given to the referee. However, this will be impossible for B and she/he can only claim that she/he has completely removed her/his signature.

Therefore the referee can conclude one of the following:

1. B tells the truth and A, apart from having supposedly destroyed B's signature in O, has also managed to luckily discover some string in O' (B's "original") and then interpret it as the adjacency matrix of a graph of which A has also discovered a 3-coloring *before* the execution of the protocol.
2. A tells the truth, having shown a hard to compute property of a string that was embedded in O' and B has not managed to destroy this signature.

The first conclusion, if true, would lead the referee to attribute the ability to exhibit a three coloring in a graph to pure luck. However, due to the intractability of the 3-coloring problem, pure luck on A's part can be safely excluded. Therefore, the second conclusion is more credible than the first.

Finally, it is apparent that if B had somehow appropriated A's signature (e.g. by extracting it from an image or by stealing it from A's database) then B could not use the signature to impersonate A since what constitures proof of ownership is in fact the knowledge of a 3-coloring of the graph represented by the signature and not the signature string itself.

5 Application to Digital Images

In this section, an application of the aforementioned protocol is presented for use in signing digital images. The support experiments (including the development of the required tool to embed the graph in digital images) were designed in order to demonstrate that the proof of ownership protocol is applicable to digital images.

A digital image is modeled as an $m \times l$ matrix, where the position $[i, j]$ represents a pixel or a basic unit of an image. Since RGB images are considered, each position is actually a vector (x, y, z), where each of the components defines the values of the Red, Green and Blue channels respectively. The image is, thus, considered as a set of 24 $m \times l$ binary matrices (8 $m \times l$ binary matrices for each color). The blue channel is decomposed into 8 bit-levels by assigning a bit to a different level: Level 1 (MSB - most significant bit), Level 2, $\ldots$ Level 8 (LSB - least significant bit).

As outlined in Section 4, a signature (3-colorable graph) is embedded in digital works in order to provide proof of ownership. There are several methods that may be used to embed the signature that are broadly classified as *spatial domain* and *frequency domain* (see [7, 18, 2]) with various degrees of robustness against attacks for signature destruction or removal. The method that was adopted works in the spatial domain for simplicity and is based on a particular characteristic of the Human Visual System according to which the human eye is less sensitive to changes occuring in the blue color. Thus, in the implementation, the graph was embedded in the least significant bits of the blue channel values of the target image.

The 3-colorable graph can be represented by its adjacency matrix M. This is an $n \times n$ zero-one matrix whose $[i, j]$ position $(i, j = 1, \ldots, n)$ contains 1 if vertices v_i and v_j are adjacent in the graph, otherwise it contains a 0. The matrix M is symmetric and its main diagonal contains all zeros (0s) as the graphs are undirected and there are no loops. Therefore, it was only necessary to embed in the image $n(n-1)/2 - n$ bits. These bits form a binary image and they can be embedded in positions whose coordinates are generated by a suitable pseudorandom number generator. Doing so, the image stays almost intact and the graph is imperceptible by a human observer.

In the extraction process, the inverse procedure is applied where the bits embedded in the LSB of the blue channel are extracted using the same pseudorandom generator with the same key that was used for the embedding process. The recovered bits are then treated as the adjacency matrix of a graph. Then for debates over the image's ownership, the ZKIP described in Section 4 can be used along with the rightful owner's knowledge of a 3-coloring of the resulting graph. As far as the quality of the embedding is concerned, experiments conducted with embeddings of adjacancy matrices of random graphs of 1000 vertices show that the resulting images exhibit an average PSNR greater than 50dB. These preliminary results show that it is possible to embed a *large* amount of data into an image preserving, at the same time, the quality of the image and the imperceptibility of the embedded signature.

6 Conclusions and Future Research

This work proposed the use of signatures whose usefulness depends not on the knowledge of the signature itself (i.e. the particular string of bits) but on the *knowledge* of a hard to guess characteristic of it. In particular, signatures were considered that represent the adjacency matrices of graphs constructed so as to possess a particular coloring and belong to the "hard instances" region of graphs. The main point behind this proposal is that since it is computationally difficult to find such a coloring without knowning in advance, a person who can exhibit such a coloring can be safely considered as the rightful owner of the signature and, consequently, of any piece of digital work that contains it.

Then the general scheme was applied to digital images, with large signature graphs embedded in the LSB of the blue channel. While this embedding process was easy to implement and allowed a quick test of the feasibility of embedding large 3-colorable graphs in an image, it is nevertheless, not particularly robust to attacks. As a future goal, it will interesting to treat the graph as a binary image, where black pixels correspond to zeros of its adjacency matrix, and white pixels to ones. Then some recent results of Chae et al. ([4]) can be used, which demonstrate that it is possible to embed large gray scale images in color images so that the quality of the embedded image remains high when it is extracted, even if the signed image is subjected to up to 75% wavelet compression and 85% JPEG lossy compression.

According to Craver et al. ([8]), invisible signatures/watermarks can not resolve rightful ownership in current signature/watermarking schemes, where "current" refers to techniques introduced since 1996. Indeed it is obvious that without a standardization of authentication techniques anyone can claim ownership of an image. However, in order to proceed with such a standardization the scientific community must be convinced of the effectiveness of a proposed technique. The work presented in this paper moves along the lines of such a standardization by proposing the use of signatures representing combinatorial objects (e.g. 3-colorable graphs) with a particular *hard to compute* characteristic (e.g. 3-coloring) known *only* to the rightfull owner of the signature. Then in view of the difficulty of discovering this characteristic, and in this respect results of the study of threshold phenomena in hard combinatorial problems are very useful, knowledge of the characteristic could potentially be *formally* agreed upon to coincide with *rightfull ownership.*

References

1. D. Achlioptas, C. Gomez, H. Kautz, and B. Selman, Generating satisfiable problem instances, *in Proceedings of AAAI 2000*, 2000.

2. S. Armeni, D. Christodoulakis, I. Kostopoulos, Y. Stamatiou, M. Xenos, A Transparent Watermarking Method for Color Images, *First IEEE Balcan Conference on Signal Processing, Communications, Circuits, and Systems*, June 2000, Istanbul, Turkey.
3. W. Bender, D. Grul, N. Morimoto, and A. Lu, Techniques for data hiding, *IBM Systems Journal*, Vol. 35, NOS 3 & 4, 1996.
4. J.J. Chae, D. Mukherjee, and B.S. Manjunath, Color image embedding using multidimensional lattice structures, *in Proceedings of the IEEE International Conference on Image Processing*, Chicago, Illinois, Vol. 1, pp 460–464, October 1998.
5. P. Cheeseman, B. Kanefsky, and W.M. Taylor, Where the really hard problems are, *in Proc. of the International Joint Conference on Artificial Intelligence*, Vol. 1, pp 331–337, 1991.
6. S. Cook and D. Mitchel, Finding hard instances of the satisfiability problem: A survey, *in Satisfiability Problem: Theory and Applications*, DIMACS series in Discrete Mathematics and Theoretical Computer Science **25**, 1–17, American Mathematical Society, 1997.
7. I.J. Cox, J. Kilian, F.T. Leighton, and T.G. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, 6(12):1673-1687, 1997.
8. S. Craver, N. Memon, B.-L. Yeo, and M. Yeung, Can invisible watermarks resolve rightful ownerships?, *IBM Research Report*, RC 20509, 1996.
9. S. Craver, Zero knowledge watermark detection, *3rd International Workshop on Information Hiding (IHW 99)*, 1999.
10. E.R. Dougherty, Random processes for images and signal processing, *SPIE/IEEE Series on Imaging Science & Engineering*, 1999.
11. A. Fabien, P. Peticolas, R.J. Anderson, and M.G. Kuhn, Information hiding-A survey, *IEEE special issue on Protection of Multimedia Content*, 87(7), pp. 1062–1078, July 1999.
12. M.R. Garey and D.S. Johnson, *Computers and Intractability, a Guide to the Theory of NP-Completeness*, W.H. Freeman and Company, 1979.
13. R. Gonzalez and R. Woods, *Digital Image Processing*, Addison Wesley, 1992.
14. B. Hayes, Computing Science: Can't get no satisfaction, *American Scientist*, March–April, 1997.
15. K. Hirotsugu, An Image Digital signature system with ZKIP for the graph isomorphism, *International Conference on Image Processing (ICIP)*, 1996.
16. S. Katzenbeisser, A. Fabien, and P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech House Books, 1999.
17. S. Kirkpatrick and B. Selman, Critical behavior in the satisfiability of random boolean expressions, *Science* 264, pp 1297–1301, 1994.
18. M. Kutter, F. Jordan and F. Bossen, Digital Signature of Color Images using Amplitude Modulation, *Journal of Electronic Imaging*, Vol. 7, No. 2, pp. 326-332, April 1998.
19. F. Massacci and L. Marraro, Logical cryptanalysis as a SAT problem: the encoding of the Data Encryption Standard, manuscript, 1999.
20. C.H. Papadimitriou, *Computational Complexity*, Addison-Wesley, 1994.
21. R.B. Wolfgang and E.J. Delp, Overview of image security techniques with applications in multimedia systems, *in Proceedings of the SPIE Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways*, Vol. 3228, pp. 297–308, Dallas, Texas, 1997.