Using Robust Hash over DIGITA Watermarking for Message Authentication

Jyoti Rajput[1], Kalyankar.P.P[2] & Anjalidevi[3]

Abstract- **Authentication is the process of insuring that both ends of the connection are in fact who they say they are. This applies not only to the entity trying to access a service but to the entity providing the service, as well such as a file server or Web site. Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well. While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications. In the concept of networking and data security, often when two parties communicate over a network, they have two main security goals: privacy and authentication. In fact, there is compelling evidence that one should never use encryption without also providing authentication. Many solutions for the privacy and authentication problems have existed for decades, and the traditional approach to solving both simultaneously has been to combine them in a straightforward manner using so-called "generic composition." However, recently there have been a number of new constructions which achieve both privacy and authenticity simultaneously, often much faster than any solution which uses generic composition. In this proposed project, a secure approach is mechanized for ensuring both privacy and authenticity, the so-called "Authenticated Encryption" problem.**

Keywords: **Authentication, Encryption, DCT, HASH**

1. *College of Engineering Osmanabad*
jyotirajputpawar@rediffmail.com

2. *College of Engineering Osmanabad*
kalyankarpravin@rediffmail.com

3. *VVP Institute of Engg & Tech., Solapur*
anjali2_devi@yahoo.co.in

I. Introduction

Advances in modern computing technology, ranging from faster processors to expanded memory to new storage devices, have brought certain applications into mainstream use. For example, non-linear digital video editing has become practical on a large scale since compression algorithms, system microprocessors and graphics processors have advanced enough to cope with the massive volumes of video data involved. Similarly, data encryption has been available for a number of decades, but practical applications have been largely restricted to high-end systems in the banking, military and scientific sectors. In recent years, these restricted uses have been overcome by the greater availability of desktop and notebook computers that compare favorably to supercomputers of years past. Currently, state-of-the-art techniques capitalize on the features in business and personal computer systems and deliver the data security benefits of encryption to everyday users. Modern systems can routinely encrypt and decrypt data in the background using 128-bit (or larger) keys and advanced algorithms while causing minimal, nearly imperceptible effects on performance. Problems that limited the usefulness of past-generation encryption tools have been largely overcome by enhanced application designs, improved deployment processes, better maintenance tools, more efficient algorithms and standards-based architectures that simplify integration of encryption solutions with network infrastructures.

Thesecurity mechanisms which are employed to protect the multimedia data from unauthorized operations are (a) Multimedia encryption to prevent eavesdropping,

(b) Watermarking for copyright protection and tracking (c) Parametric multimedia hashing for content authentication[1]. The hash functions are one-way functions, which return a fixed length result H(M) when they are applied.

on an arbitrary length message M.The one-way hash functions respect the following properties [9], [10]:

1.If the message M is given, it is easy to compute H(M);
2. It is hard to find the message M if H(M) is given;
3. If a message M is given, it is hard to find another message M', such that H(M) = H(M');

4. It is hard to find two random messages M andM', such that H(M) = H(M');.

It is easy to implement the hash function in hardware and in software[2].

Despite the advances in encryption techniques and vastly improved computer capabilities, many of the fallacies and outdated understandings about encryption persist. Sometimes these myths are even being perpetuated in popular technology publications where some authors and editorial staff fail to do their research thoroughly.

While the implementations differ and the tools vary widely, the fundamentals of encryption are strikingly similar for most applications. Companies collaborate more freely and more often with partners and suppliers, responding to supply chains that now stretch across the world. Web-based business processes and e-commerce have combined to create a much more open IT infrastructure and corresponding protections must be put in the place to counteract possible network vulnerabilities. The ubiquitous portable computing devices in use by employees often contain sensitive data that must be shielded from prying eyes in the event of loss or theft of the device.

Strong encryption provides a powerful mechanism that can be applied to many parts of an organization's data security practices, offering effective, continuous protection of data. This protection can encompass a range of uses, from end-point devices in the field to the core of the central servers where vital information resides. Hence reading the above comments about significance of data encryption, the proposed system furnishes following uniqueness that can be considered as importance of the topic:

a)The proposed project is much advanced than Steganographic technique. Steganographic techniques uses data embedded inside image using either public or private key. But the proposed system will not only user user-defined public key, but also it will deploy hash function in image format that is quite impossible to break.

b)The proposed project is highly flexible and secure version of conventional cryptographic technique where they (conventional techniques) needs to manage a massive key management protocols. The proposed system is light weight as the hash value extracted from image file is only 100 bits in size.

c)The mechanism of the proposed system is quite unique compared to conventional system. The proposed system performs encryption on each block of images (16x16 block) using Discrete Cosine Transform. The technique is highly robust and renders almost impossible for any attacker to perform decryption.

II. Digital Watermarking

The goal of the digital watermarking is the copyright protection in order to prevent the unauthorized copying of the digital multimedia data. Another solution for the data protection consists in using the cryptography, but this approach has a major disadvantage. The multimedia data is protected by encryption only during the transmission time and after that they will be stored in their original form (as plaintext) which permits to any intruder to have an access to them. In case of digital watermarking, if the watermark is inserted in an image or in a video sequence, it will remain permanently in that data .The watermark can be either visible or invisible

The invisible one is more efficient because it is spread over the entire video not only on a certain part of it (like in the case of the visible one), therefore it is harder to be removed. It acts like a label that contains information about the owner, the user, the number of copies, etc. The watermark insertion process must respect the following requirements: invisibility – the inserted watermark must remain imperceptible to the human visualsystem; security – its extraction must be impossible for any unauthorized person even if the insertion algorithm is public; robustness – the watermark intentional or unintentional removal should be impossible without damaging the original data. In order to respect these requirements, the secret must lie in the pseudo-noise generation key. To increase the security and the robustness of the system, non-oblivious watermarking schemes are used [4]. In this case, the watermark depends on the original signal and it will be unfeasible to conduct a forgery because there is no access to the unmarked data, which is kept secret. The watermarking process can be done in the spatial domain [3],[7] or in the transform domain (e.g. DCT)[1].

What is needed in both applications discussed above is a watermark W that depends sensitively on a secret key K and continuously on the image I:

1. $W(K, I)$ is uncorrelated with $W(K, I')$ whenever images I and I' are dissimilar;

2. $W(K, I)$ is strongly correlated with $W(K, I')$ whenever I and I' are similar (I' is the image I after an attack comprising of a rotation, scale, and grayscale modifications);

3. $W(K, I)$ is uncorrelated with $W(K', I)$ for $K \neq K'$.

So, we have to look for a watermarking-encryption dual in which the watermark remains invariant to the encryption process. Let the original media be P, the encryption process be represented as E , the watermark embedding algorithm be represented as W_{embed}, watermark extraction

algorithm be represented as $W_{extract}$, the watermark be W, the watermark key be K_w, the encryption key be K, watermarked media be P_w then mathematically,

$E(W_{embed}(P,W,K_w),K) = E(P_w,K) = P_{w,encrypt}$ (1)

We want the watermark to remain invariant to the encryption process. That is to say, we want a scheme wherein we can extract the watermark without decrypting the received data. Mathematically,

$W_{extract}(P_{w,encrypt},K_w) = W$ (2)

If such a scheme is achieved, it will be possible to extract the watermark directly from the encrypted media. The watermark can be embedded directly in the encrypted domain. Zero knowledge proof will be achieved. In order to extract a watermark and embed a new one, one will not have to go through the decryption-watermark embedding-encryption triples. In [7], watermarking detection algorithm has been proposed which is able to detect the watermark irrespective of whether it is embedded in the plaintext and then the watermarked data
is encrypted or first the plaintext is encrypted and then the encrypted data is watermarked. Watermark is detected without the knowledge of the decrypting key. But, the encryption that they have used permutes only the first 25 DCT coefficients. This is a weak encryption and the encrypted image leaks some information about the original image[2].

A. Drawback in Watermarking:

Digital watermarking is a relatively young branch in the field of signal processing and information theory. Due to the nature of multimedia objects, security issues in many application scenarios are often interleaved with signal processing issues. As a result, in many previous works, security issues in multimedia watermarking are not treated in a rigorous manner. In particular, security requirements are often stated in an imprecise way using natural language, and attacker models are often too simplistic. This makes it very difficult to assess the security of the schemes when, in real life, the attackers are very creative intelligent[3][20][21].

To understand the security issues in multimedia watermarking and to design secure schemes, the most important task is to define what security is in the application scenarios. In a particular application, our security concerns usually consist of two parts: (1) The security requirements (i.e., the goals we want to achieve), and (2) the attacker model (i.e., the type of attackers we are dealing with). In essence, when we say that a system is secure we should clearly mean that the system is able to meet some security requirements in the presence of certain type of attackers.

Moreover, identification on the basis of watermarks can operate in a stand-alone environment: nothing more than some basic watermark (public or secret) keys are needed to retrieve identity. But recently, an old technique, in this paper referred to as robust or perceptual hashing, has re-emerged as a viable alternative. This has come about due to two reasons. Firstly, there has been considerable progress in boosting performance. Secondly, there is the realization that the use of watermarking for content recognition actually amounts to adding redundancy.

A quick scan of the available literature shows that the majority of papers have images as their target i.e. audio-visual object[21][22][24]. The number of publications on audio and video watermarking is growing, but the difference in numbers is significant. What is also apparent from a literature scan is that the main target application is copyright protection or copy protection. This observation explains the great interest in the security aspect of watermarking, and a large number of publications therefore focus on intentional attacks and their countermeasures[20]. This silent assumption between security and watermarking is also reflected by the effort put into designing attack tools and the title of a number of conferences (e.g. “Security and Watermarking of Multimedia Content”, San Jose). Also the two main industrial applications of watermarking have a focus on security. Whether or not this strong perceived relationship between security and watermarking is beneficial to the deployment of watermarking remains to be seen[1][5][6].

III. . Invariant Hash:

Hash functions are frequently called message digest functions. Their purpose is to extract a fixed-length bit string from a message (computer file or image) of any length. Obviously, a message digest function is a many to-one mapping. In cryptography, hash functions are typically used for digital signatures to authenticate the message being sent so that the recipient can verify that the message is authentic and that it came from the right person. The requirements for a cryptographic hash function are [1]

- Given a message m and a hash function H, it should be easy and fast to compute the hash $h=H(m)$.
- Given h, it is hard to compute m such that $h=H(m)$ (i.e., the hash function should be one way)
- Given m, it is hard to find another message m' such that $H(m')=H(m)$ (property of being collision free)

From the above properties it is clear that hash functions are "infinitely" sensitive in the sense that a
small perturbation of the message m will give you a completely different bit-string h.

In applications involving digital watermarking and authentication of digital images, the requirements on what should be a digest of an image are somewhat different. Changing the value of one pixel does not make the image different or non-trustable. Distortion introduced by lossy compression or typical image processing does not change the visual content of the image. What would be useful to have is a mechanism that would return approximately the same bit-string for all similar looking images, yet, at the same time, two completely different images would produce two uncorrelated hash strings. This is what we call in this paper a robust hash function (visual hash). One can say that we want approximately the same hash bit-strings for two images whenever the human eye can say that these two images "are the same". Obviously, this is a challenging problem that can never be solved to our complete satisfaction. This is because the fuzzy concept of two images being visually the same is inherently ill defined and difficult, if not impossible, to grasp analytically. For example, changing one pixel in the pupils of a person's eye is for all purposes a negligible change. But once we change the color of every pixel in the pupil from, say, blue to brown, an important personal characteristic has been changed. Thus, we would conclude that the two images are no longer the same. However, the pupils can occupy a very small part of the image and our robust hash, not knowing the importance of eyes, may return the same hash bit-string. Being aware of these and other limitations, nevertheless, in this paper, we attempt to meaningfully define the concept of a robust visual hash. Before we start with the definition and ideas how to construct such a function, we give a brief introduction into oblivious digital watermarking and explain how robust hash will play an important role in specific watermarking applications, such as authentication and fingerprinting [3].

Roubust Hashing: From the definition given in the previous section, robust image hash is a bit-string that somehow captures the essentials of the digital image or block. Our requirement is that we need a key-dependent function that returns the same bits or numbers from similar looking images. So, the question is: "What is preserved under typical image processing operations?" Image edges typically contain the essence of an image. We could also use some relative relationship between pairs of image features, such as DCT coefficients. Also, it is well known that the principal directions and principal values calculated from image blocks are resistant to all kinds of grayscale image processing [11]. However, the principal directions are publicly known and the hash built from them would not have any security element in it. One could introduce a key-dependent linear or nonlinear combination of the values determined from singular value decomposition of the image block, but this would provide only marginal security since the main robust values are not protected by a key, and therefore, can be intentionally manipulated. Another possibility would be to use invariant moments [12] or their key-dependent combinations for robust extraction of bits. Again, the problem with this approach is that the invariant moments are publicly known and can be purposely modified. Thus, the watermarking technique that utilizes bits derived from those moments would be inherently less secure. In [13], the authors proposed the usual hash of an edge map of a scaled-down image as a robust way of getting key-dependent hash bits for images. The logic is that edges are salient features of images and should be preserved for most image transformations. However, the usage of the cryptographic hash function will create a cliff-off effect that may not be desirable for robust watermarking. As long as the edge map does not change (after thresholding), the hash behaves in a robust manner with respect to small noise adding. However, once the edge map is modified, even in one pixel only, the hash returns a completely different bit-string. It would be nice to have a robust hash that deteriorates gradually rather than in an abrupt way, so that the watermark built from the hash is still highly correlated with the watermark used in watermark embedding. Another approach that works quite well for small distortion especially distortion introduced by JPEG compression was introduced in [14]. The authors emphasize the fact that the mutual relationship of DCT coefficients in 8□8 blocks will be preserved no matter what quantization matrix is used for coding the image. Thus, one can extract one bit of information from predetermined pairs of DCT coefficients based on the fact if the first or the second pair member is larger than the other. The extracted bits are finally processed using a one-way function to obtain the final hash. There are several disadvantages of this method for use as a robust hash. First of all, while this method works very well for JPEG compression, its performance is less satisfactory for a different type of distortion, such as contrast enhancement. Second, as long as the mutual relationship of the coefficient pairs is not changed, the authentication technique based on this hash will not detect the change. And finally, one can purposely modify certain DCT coefficients to change the hash completely while making undetectable modifications to the image. This is because the DCT coefficients that enter the one-way function are publicly known.

Using the standard form of the discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The dct2 function computes the two-dimensional discrete cosine transform (DCT) of an image. The DCT has the property that, for a

typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. For example, the DCT is at the heart of the international standard lossy image compression algorithm known as JPEG. (The name comes from the working group that developed the standard: the Joint Photographic Experts Group.)

The two-dimensional DCT of an M-by-N matrix A is defined as follows.

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

The values Bpq are called the DCT coefficients of A. (Note that matrix indices in MATLAB always start at 1 rather than 0; therefore, the MATLAB matrix elements A(1,1) and B(1,1) correspond to the mathematical quantities A00 and B00, respectively.)

The DCT is an invertible transform, and its inverse is given
by

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

The inverse DCT equation can be interpreted as meaning that any M-by-N matrix A can be written as a sum of MN functions of the form

$$\alpha_p \alpha_q \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

These functions are called the basis functions of the DCT. The DCT coefficients Bpq, then, can be regarded as the weights applied to each basis function. For 8-by-8 matrices, the 64 basis functions are illustrated by this image.Horizontal frequencies increase from left to right, and vertical frequencies increase from top to bottom. The constant-valued basis function at the upper left is often called the DC basis function, and the corresponding DCT coefficient B00 is often called the DC coefficient.

A) Drawback in hashing:

On the other hand, the security of hashing system is based upon the correspondence between perceptual similarity and hash values. For most basic perceptual hashing techniques the similarity of hash values is sign of perceptual similarity, but it need not be the other way around. This is a weakness that can be exploited in security applications. For example, a hashing technique in a Napster-like context that is not robust to time-scale modifications will make a very insecure filtering mechanism. Ultimate security can be obtained with a perfect perceptual hashing technique, i.e. a hashing technique where perceptual similarity is completely captured by the perceptual hash function[10][21][22][23].

- Majority of the prior research work are found to suffer one or more of the following problems that may have a serious negative impact on a given application:
- Insufficient security
- Decrease in the compression performance of entropy coding
- Insignificant computational reduction with respect to total encryption
- Lack of bit stream compliance & Increase in key size.

IV Results

To, show the expected results it is tested across a variety of images for two reasons:

- The hash value should be unique to a given image. Because Different images should yield significantly different hash values.
- If the distance between hash values from two different images are significantly different, this can be used as a means of indexing the respective images.
- The hash invariance to encryption must be verified for different images in order to justify this generalization.
- First we compute the 16 × 16 block DCT. Then, each block is encrypted.
- The key K decides the values of p, q and the number of times. The security is strong because not only the parameters p and q are decided by the key but we also have randomized the number of iterations for the picture.

- The next step is to calculate the hash value of the original image and its corresponding encrypted version. As expected, they are found to be the same.
- The hashes obtained for each of the images is of 100 bits length. They are shown in the form of images of dimension 10×10 .
- We also verify that the hash for each image obtained from the proposed algorithm is unique.

The hashes obtained from the proposed algorithm. These hashes remain transparent to the encryption process. To verify experimentally by finding out the hash of the original image and the encrypted image. Also, the hashes obtained from two different encrypted versions (same encryption algorithm but different keys used) of the same original image remain equal.

The proposed work may get these probable results The calculations are done both for the plain text data as well as the encrypted data and the resultant hashes are found to be the same as shown in Fig2[2].

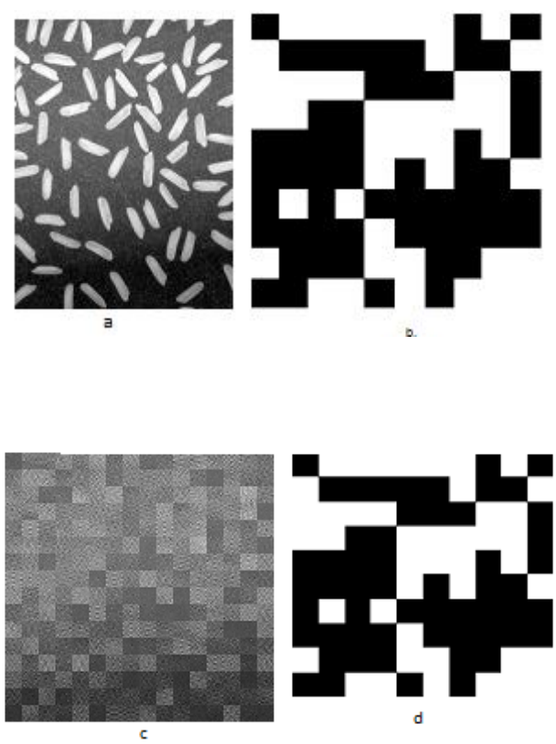

Fig 2 Results showing the validity of the proposed algorithm. The hash of the original image and the encrypted image are same.(a) Original Rice image, (b) Hash derived from Original Rice image, (c) Encrypted Rice image, (d) Hash derived from Encrypted Rice image.

V Conclusion

The message authentication codes and also the method of encoding are treated as vertical security method, wherever message authentication codes are deployed to confirm knowledge credibility whereas encoding is employed to preserve confidentiality. During this proposed project work, a framework is introduced that uses hash value of an encrypted image that is intended to be identical because the hash value of the parent unencrypted original image. Since the hash price is computed while not decrypting the initial knowledge, one will prove credibility while not truly revealing the knowledge. The prime intention of the project work will be to formulate the problem of authenticating encrypted information and design of a non-complicated and light weight hashing algorithmic rule applicable to encrypted images. We plan to use these two features to construct the hash value. We may make further additions if time permits.

References:

[1] B. Schneier, ***Applied Cryptography***, John Wiley&Sons, New York, 1996.

[2] Robust Hash Functions for Digital Watermarking Jiri Frindrich and Miroslav Goljan

[3] Digital Image Watermarking Using The Discrete Cosine Transform And The MD5 Cryptographic Hash Function Wahyu Prakosa Adi & Volker Müller Duta Wacana Christian University

[4] Kashyap, S.; Karthik, K. **Authenticating Encrypted Data** Communications (NCC), National Conference on 2011 Year: 2011, Page(s): 1 – 5

[5] J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *Proc. Int. Conf. on Information Technology: Coding an Computing*, pp. 6–10, March 2000.

[6] E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of image alterations using semi-fragile watermarks," in *SPIE Intl. Conf. on Security and Watermarking of Multimedia Contents II*, Jan 2000.

[7] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[8] S. Lian, "Quasi Commutative Watermarking and Encryption for Secure Media Content Distribution," *Multimedia Tools Appl, Springer*, vol. 43, pp. 91–107, 2009.

[9] S.Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative Watermarking and Encryption for Media Data," *OE Lettters, SPIE*, vol. 45(8), 2006.

[10] G. Boato, V. Conotter, F. G. B. D. Natale, and C. Fontanari, "A joint asymmetric watermarking and image encryption scheme," in *Proceedings of SPIE Electronic Imaging*, vol. 6819, pp. 601–602, 2008.

[11] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct 1949.

[12] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals, Elsevier*, pp. 749–761, 2004.

[13]]Z. Lv, L. Zhang, and J. Guo, "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed DynamicsSystem," *Proc. Of Second Symposium on Computer Science and Computational Technology*, pp. 191–194, 2009.

[14] Hugo Krawczyk, The Order of Encryption and Authentication for Protecting Communications (Or: How Secure is SSL?)?, Proceeding CRYPTO '01 Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology Pages 310 – 331, 2001

[15] Charanjit S. Jutla, Encryption Modes with Almost Free Message Integrity, Proceeding EUROCRYPT '01 Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology Pages 529 – 544, 2001

[16] Phillip Rogaway, Mihir Bellare, John Black, OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption, ACM Journal Name, Vol. V, No. N, M 2003, Pages 1–3

[17] Yuliang Zheng, Digital Signcryption or How to Acheieve Cost (Signature & Encryption)<<Cost(Signature)+Cost(Encryption), CRYPTO, 1997

[18] Qiming Li, Nasir Memon, Husrev T. Sencar, Security Issues in Watermarking Applications A Deeper Look, In *ACM Workshop on Multimedia Content Protection and Security*, Santa Barbara, CA, October 2006

[19] Ton Kalker, Jaap Haitsma, Job Oostveen, Issues with Digital Watermarking and Perceptual Hashing, Date: 12 November 2001, ISBN: 9780819442420