Overview of Watermarks, Fingerprints, and Digital Signatures

Sonali V. Satonkar , Dr. Seema Kawathekar
Dept. of Computer Science and Information Technology
Dr. BabasahebAmbedkarMarathwadaUniversity,Aurangabad

Abstract: Growing concern the world over, related to personal and property safety has propelled rapid growth of security and surveillance related technologies. The biometric system is one such that can provide accurate and reliable scheme for person verification. The main aim . Introduction of fingerprint,introduction watermark, & digital signatures. .[1]

Keyword: cryptography, Watermarking, public-key cryptosystems**.**

Introduction: While the rapid development and deployment of new IT technologies has improved the ease of access to digital information, it has also led to fears that copyright could be eroded by the illegal copying and redistribution of digital media. This is of particular concern, for example, to commercial publishers of digital audio and video content whose existence depends on defending the copyright of their information assets. If content owners cannot be assured that they will be properly compensated for use of their works, they will be unlikely to make these available for access over public networks. Mechanisms to protect content are seen, therefore, as a necessary step towards the creation of a global commercial information infrastructure.

While equipment capable of copying audio, video, and text content has long been available for domestic use, the loss of quality that analogue copying entails, and the labour involved in the physical process of copy production has acted to limit copyright abuse. With digital media, however, perfect copies can be produced and distributed with little effort, and modern compression algorithms have reduced the safeguard once possessed by digital content by virtue of its sheer size.

Some technologies (such as watermarking and fingerprinting) are emerging that attempt to provide copyright owners with the desired degree of protection, and to act as a disincentive to data piracy. Others, such as digital signatures, are familiar from cryptography, and provide services for origin authentication and content integrity. [1]

In brief, the three technologies under consideration in this paper can be described as follows:

a) Watermarking: A technique for embedding hidden data that attaches copyright protection information to a digital object. This provides an indication of ownership of the object, and possibly other information that conveys conditions of use.

b)Fingerprinting: A type of watermark that identifies the recipient of a digital object as well as its owner (i.e. a 'serial number' assigned by the vendor to a given purchaser). This is intended to act as a deterrent to illegal redistribution by enabling the owner of the data object to identify the original buyer of the redistributed copy.

c)Digital signatures: A mechanism employed in public-key cryptosystems (PKCS) that enables the originator of an information object to generate a signature, by encipherment (using a private key) of a compressed string derived from the object. The digital signature can provide a recipient with proof of the authenticity of the object's originator.

Watermarking Technique: The purpose of watermarks is two-fold: (i) they can be used to determine ownership, and (ii) they can be used to detect tampering. There are two necessary features that all watermarks must possess. First, all watermarks should be detectable. In order to determine ownership, it is imperative that one be able to recover the watermark. There are essentially two mechanisms by which a watermark can be recovered.

Incomplete watermarks can only be recovered provided the original image is available. Complete watermarks can be recovered regardless. Complete watermarks are more desirable as they apply to a broader spectrum of applications. When watermarking large files or a large number of files in a database, complete watermarks are preferable as they make it unnecessary to store multiple copies of the original (unwatermarked) file. Second, watermarks must be robust to various types of processing of the signal (i.e. cropping, filtering, translation, compression, etc.). If the watermark is not robust, it serves little purpose, as ownership will be lost upon processing. However, havingsome built-in fragileness can be useful at times. If fragile watermarks are used and the data is altered, the watermark can pinpoint the areas that were changed. Fragile watermarks can detect minor changes or tampering of data. Robust watermarks on the other hand,are useful for detecting large-scale attacks on data[2].

Watermarking application areas: Watermarking techniques may be relevant in the following application areas

a) Applications that convey ownership assertions: The primary use of watermarking is where an organization wishes to assert its ownership of copyright for digital objects. This is of great interest to 'big media' organizations, and of some interest to other vendors of digital information, such as news and photo agencies.

These applications require a minimal amount of information to be embedded, coupled with a high degree of resistance to signal modification (since they may be subjected to deliberate attack).

b) Collaborative copy protection applications: Some schemes have attempted to satisfy more complex copy protection requirements. An early example is the serial copy management system (SCMS), introduced in the 1980s, which enabled a user to make a single digital audio tape of a recording they had purchased but prevented the recording of further copies (i.e. second generation) from that first copy. The scheme failed ultimately because not all manufacturers of consumer equipment were prepared to implement the scheme in their products.

More recently, a working group representing mediand consumer electronic manufacturers, has attempted to agree a copy management scheme for the digital versatile disc (DVD). This is intended to enable a consumer to make copies of his home videos without restriction, to permit single-generation recording of broadcast programmes (for time shifting), but to prohibit copying of purchased media.

c) **Applications requiring data integrity check***s*: In these applications, it is necessary to have assurance that the origin of a data object can be demonstrated and its integrity can be proved. One example is photographic forensic information that may be presented as evidence in court. Given the ease with which digital images can be manipulated (as the newspapers demonstrate daily) there is a need to provide proof that an image has not been altered. Such a mechanism could be built into a digital camera

Watermarks are not particularly effective in assuring data integrity, in that they are usually resilient only to small changes in the data object (cropping, tone-scale correction) and are invalidated by large changes (such as the removal of a figure from an image). Indeed, there is some doubt whether any data-hiding technique will be sufficient for an application that requires data integrity. In cases where proof of data integrity is required, only PKCS mechanisms, which are intolerant of any transformation of the marked object, will provide this level of security.

Annotation applications: In this applications area, watermarks convey object-specific information ("feature tags" or "captions") to users of the object. For example, individual features in a still image might be labelled, and the whole image given a caption. This may be used to attach patient identification data to medical images, or to highlight regions of diagnostic significance. These applications require relatively large quantities of embedded data. While there is no need to protect against deliberate tampering, normal use of the data object may involve such transformations as image cropping, or scaling, and will require the use of a technique that is resistant to those types of modification. [1]

Watermarks & Fingerprint:Digital watermarks are intended to confer properties on digital objects similar to those that traditional watermarks confer on printed objects. Paper watermarks were first produced in the manufacturing process from the pattern of the mould left when paper slurry is pressed between frames to expel moisture. These have been used at various times to record the manufacturer's trademark and certify the composition of the paper. Today, most countries use watermarked paper for printing currency, to act as a safeguard against forgery. While this does not provide foolproof protection, it makes forgery that much more difficult.

With the growth in the importance of digital media, accessed over computer networks, much interest has been shown in the development of techniques for embedding digital data in information objects to convey copyright information. The technology is relatively immature, and the extent to which it can satisfy this requirement is not yet proven.

A diverse range of requirements have been proposed for watermarking. For example [3]:

a) Erasing the watermark should be difficult.

b) Adding a new watermark should be difficult.

c) The watermark should survive routine transformations such as filtering, compression, resampling, cropping, channel noise, digital/analogue conversion, and other signal processing artefacts.

d) It should be proof against well-known forms of attack (e.g., collusion attacks, where multiple versions of the same content, stamped with different watermarks, are compared).

e) The watermark should be unobtrusive, and should not impede proper use of the object.

f) The watermark should be pervasive and locally contained, to permit its recovery from a small portion of the data object.

Other requirements, apparently contradictory, have been proposed that vary according to the needs of specific applications:

g) watermarks should be perceptually visible, to reduce the commercial value of a stolen data object (though it could be argued that an authenticated object will have higher street value than an object of unknown provenance);

h) watermarks should be invisible, so that a thief will be unaware that evidence of his illegal copying exists.

As with any emerging technology that is both technically attractive and commercially relevant, many workers have entered the field, proposing different analyses of requirements and different technical solutions.[1]

Conclusion: Watermarking biometric data is a still a relatively new issue, but it is of growing importance as more robust methods of verification and authentication are being used.

Acknowledgments:

We are grateful to Dr. K.V. Kale (H.O.D) and Department of Computer Science and Information Technology for providing us infrastructure. We are also thankful to Dr. Prapti Deshmukh for constant encouragement for this paper**.**

References:

[1] JISC Technology Applications Programme (JTAP) "Overview of Watermarks, Fingerprints, and Digital Signatures ",Sandy Shaw Computing Services The University of Edinburgh August 3, 1999 .

[2] Sonia Jain Department of Electrical EngineeringPrinceton University"Digital watermarking techniques: A case study in fingerprints and faces".

[3] Farid Ahmed & Ira S. Moskowitz "Composite Signature Based Watermarking for Fingerprint Authentication".

[4] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication.system using fingerprints," Proc. of the IEEE, vol. 85, no. 9, 1365-1388, 1997.

[5] B. Gunsel, U. Uludag, and A. M. Tekalp, "Robust Watermarking of Fingerprint Images," Pattern

Recognition,vol. 35, no. 12, pp. 2739-2747, Dec 2002.

[6] A. K. Jain, Umut Uludag, "Hiding Biometric Data," IEEETrans. Pattern Analysis and Machine Intelligence, vol. 25,no. 11, pp. 1494-1498, 2003.

[7]S. Pankanti and M.Y. Yeung, "VerificationWatermarks on Fingerprint Recognition and Retrieval", in *Proceedings of the SPIE/IS&T Electronic Imaging '99.*

[8]*V.S. Nalwa. "Automatic On-line Signature* Verification", in *Proceedings of the IEEE*, vol.85, pp.215-239, Feb.1997.

[9] M. Wu, E. Tang and B. Liu. "Data Hiding in a Binary Image". To appear in *ICIP '00*.

[10] M. Riezenman. "Cellular Security: better, but foes still lurk", in *IEEE Spectrum*, vol. 37, pp.39-42, 2000.

[11]C. Hsu and J. Wu. "Hidden Signatures in Images". *IEEE ICIP III '96*, pp. 223-26.