Everything You Wanted to Know About Watermarking:

From Paper Marks to Hardware Protection.

By Saraju P. Mohanty, Anirban Sengupta, Parthasarathy Guturu, and Elias Kougianos

This article presents a detailed discussion of various aspects of watermarking technologies on applications ranging from the embedding of marks in the pictorial information on paper, to hardware protection. Included in the present discussion are the general concepts, motivation for watermarking, analog versus digital watermarking, various applications of watermarking such as paper marks, currency/postal stamps, multimedia, hardware protection etc., and security and performance metrics for evaluating a watermark.

1. WATERMARKING: WHAT IS IT AND WHY IS IT NEEDED?

A mark that is covertly inserted in an entity such as a paper document or a byte stream of an image/video is called a ‘watermark’, where this secretly embedded mark represents the ‘owner’ of an entity (refer to Fig. 1). The embedded mark is expected to not degrade and to not disturb the given functionality, information, quality, or data related to entity on which it is applied. In most cases, it is also expected to be imperceptible to human perception so that it does not divert attention from the main entity. The watermark should, but does not necessarily need to, contain a relation to the entity on which it is embedded [1, 2]. As depicted in Fig.2, popular watermarking entities are paper documents, bank notes, currency, postage stamps, images, audio and video clips, computer programs, hardware devices, and chips deployed in consumer electronics devices [3, 4]. Watermarks can be of two types: (a) regular or analog watermarks, or (b) digital (forensic) watermarks. Regular watermarks have existed for centuries in various forms, but digital watermarks came into existence in the last decade or so. Digital watermarks differ from regular watermarks in terms of perceptibility to human senses; they are only perceptible to humans only after some logical processing. In most cases, regular watermarks remain easily perceptible by humans and are difficult to remove or tamper with [2] without degrading the entity.

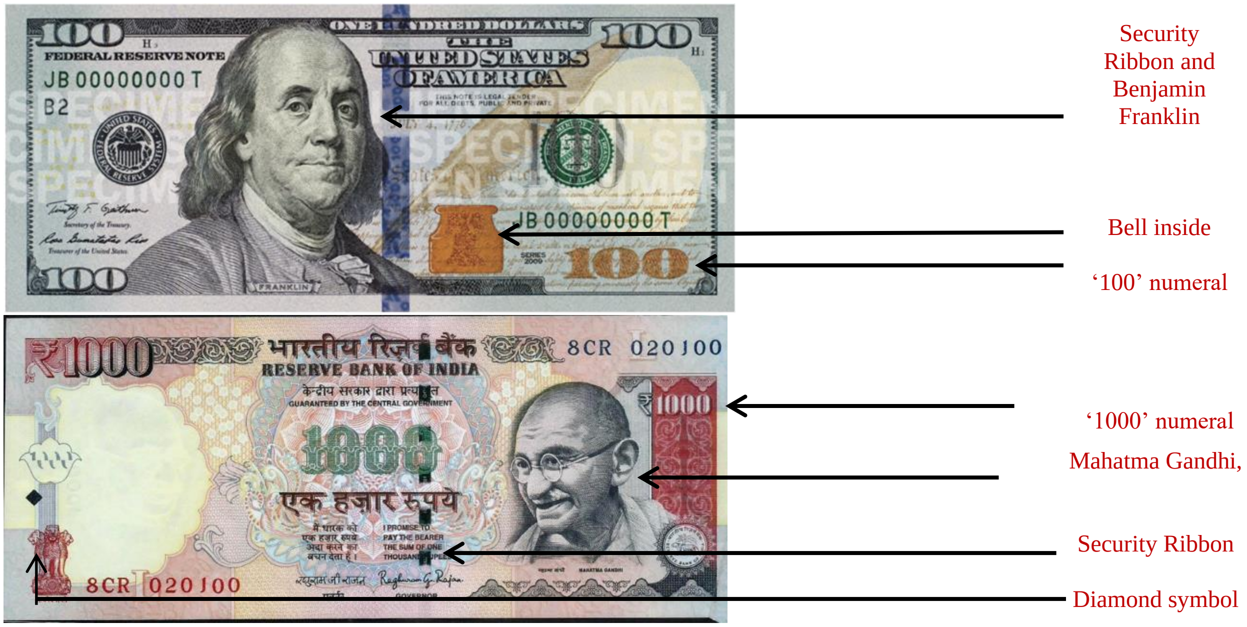


FIGURE 1. Watermarks in banknotes/currencies.

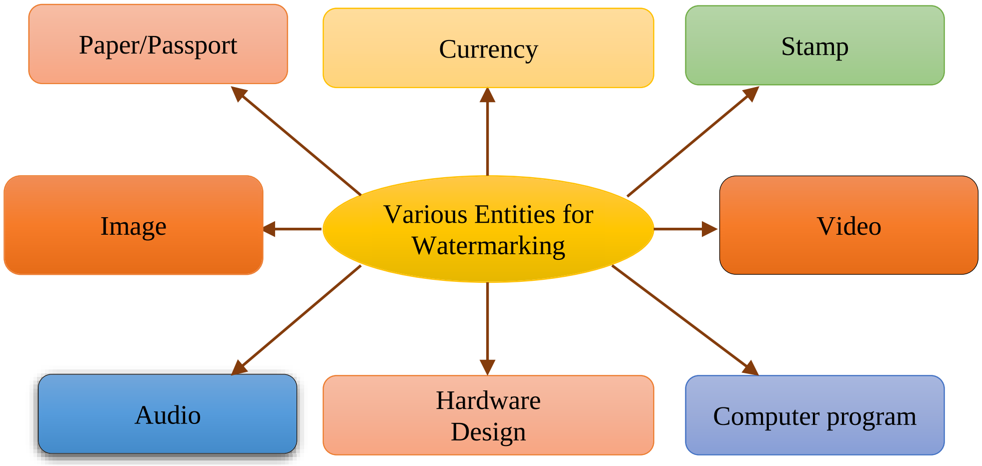


FIGURE 2. Various watermarking entities.

The term ‘watermarking’ refers to the process of embedding a hidden mark of an owner in an entity for resolving any ownership conflicts that may arise. Thus, the main goal of a watermark is to protect a genuine owner against illegal claims of ownership, illegal distribution of copyrighted works, piracy and forgery or theft. Creative entities, irrespective of their complexity, have always been susceptible to theft and copyright infringement. Hence, formal mechanisms are required to safeguard a genuine owner from external malicious attacks. It may be noted here that watermarking does not aim to prevent malicious attacks such as infringements, illegal claims of ownership, piracy etc., but provides a strong formal mechanism to track/detect such illegal activities and potentially identify the perpetrators of such activities.

2. WATERMARKING: A BROAD PERSPECTIVE

For the sake of clarity to the readers, this section presents a broad perspective of watermarking with a comparative view of several related topics including steganography, cryptography, and digital rights management (DRM).

WATERMARKING VERSUS DIGITAL WATERMARKING

Watermarking has been in existence for several centuries owing to its simplified model, low cost, and robustness. However, the advent of digital platforms rendered regular analog watermarking inadequate for protecting a genuine owner from malicious threats in various application such as audio, video, image, and hardware applications. Digital watermarking aims to hide a message (usually encoded in some form) into a digital signal without disturbing the signal itself. The digital watermark (encoded through a message) is not perceptible to human senses and is decodable only on application of some algorithm. However, regular watermarks are typically perceptible to human senses. Embedding a digital watermark is usually quite complex and requires skilled engineering knowledge, while regular watermarks are relatively easier to replicate.

WATERMARKING VERSUS STEGANOGRAPHY

Watermarking is used to verify the owner of an entity while steganography is a process of changing the entity in such a way, that only the sender and intended recipient are able to understand the message embedded in it. Sometimes steganographic codes are inside the transport layer such as an image file, document file, media files, etc. Steganography is used to hide a message in a one-to-one communication. In contrast, watermarking does the same during one-to-many communications. Similar to steganographic methods, digital watermarking methods hide information in digital media. The difference lies in the purpose of the hidden information – watermarking pertains to the digital medium itself and contains information about its author, its buyer, and the integrity of the content [5].

WATERMARKING VERSUS CRYPTOGRAPHY

The goal of cryptography is to secure the digital content being transferred over a medium. Watermarking, on the other hand, attempts to secure the owner of the digital content (by proof of ownership) but not the digital content itself. Cryptography is not capable of proving authenticity of the owner. Further, cryptography makes the message being transferred undecipherable to a third party (unintended recipient) whereas watermarking is so secretly hidden inside the content itself that the intended recipient as well as an attacker have no knowledge of how it is embedded [6].

WATERMARKING VERSUS DIGITAL RIGHTS MANAGEMENT (DRM)

Unlike watermarking, DRM techniques do not attempt to protect the owner against false claims of ownership [7]. They aim to encrypt content in such a way as not to be directly accessible (e.g., copyright protection of digital content). The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they have purchased. A secret key to decrypt the content is securely passed to authorized users, for access. Many believe that DRM techniques have failed because any content must ultimately be converted to its visible/audible form, or analog form, for a human user to perceive. Thus, when the content is reduced to an analog form, the DRM scheme of digital protection, such as encryption is removed. This is called the 'Analog Hole'. Steganography and audio/video watermarking address this problem.

As shown in Fig. 3, a digital watermark needs to have some additional desirable properties over a regular watermark [8]:

(a) **Detectability**: A watermarked message in a signal/entity (image, audio, video, hardware etc.) must be detectable to a knowledgeable user (who is aware of the encoding rules).

(b) **Signal fidelity**: Insertion of a digital watermark usually results in degradation of the signal/entity. This degradation must be kept to a minimum. In some specific domains, this degradation must be zero, which makes a digital watermark extremely difficult to embed.

(c) **Payload size:** The appropriate digital watermark depends on the size of the encoded message embedded into the signal/entity. A large size watermark message may reduce the probability of co-incidence, however concurrently increasing the probability of tampering.

(d) **Robustness**: A digital watermark must be difficult to detect by an adversary and must be fault tolerant in nature i.e., partial removal of some bits of the encoded message should still enable identification of the legal owner of the digital work. It must also be resistant to noise and malicious attacks.

(e) **Embedding cost**: A digital watermark must incur minimum design overhead in terms of resource area, delay, and power. The implementation cost should be ideally zero.

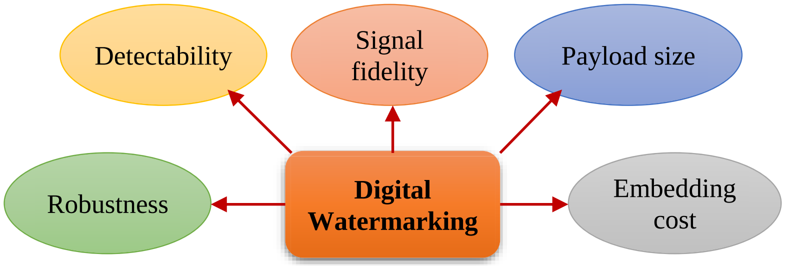
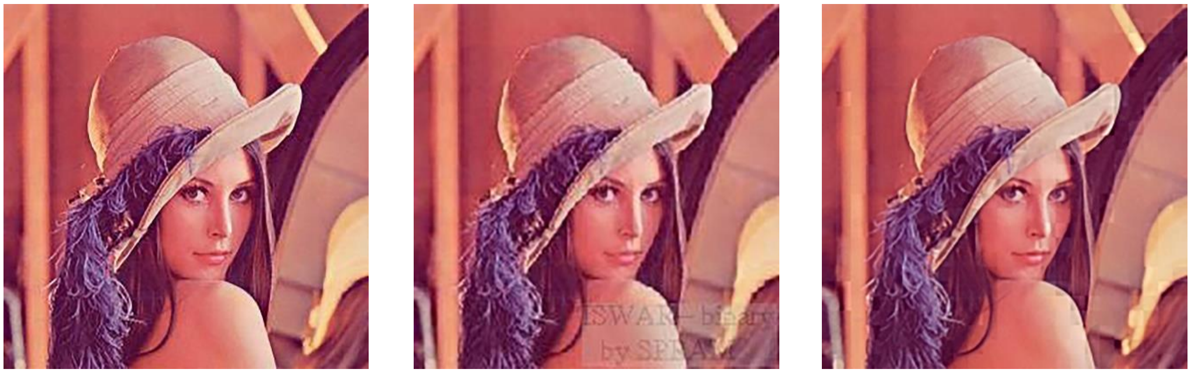


FIGURE 3. Desired properties of a digital watermark.

3. TYPES OF REGULAR AND DIGITAL WATERMARKING

Watermarking can be of multiple types:

(a) **Visible Watermarks**: This type of watermark applies to visual signals such as images and videos (refer to Fig. 4). They are transparent in nature and are imprinted onto the image. They are resistant to cropping the central portion of the image. However, the negative aspect is that they cause degradation in the image quality and allow detection through visible means (without any image processing).



(a) Original Image (b) Visible Watermarked Images (c) Invisible Watermarked Images

FIGURE 4. Visible and invisible watermarking of multimedia data [1].

(b) **Invisible Watermarks:** This type of watermark is not limited to images only. It has wide applicability to many applications. A hidden encoded message (as the watermark) which is only detectable or visible by an authorized entity through some logical processing is embedded into the data/signal/design. It allows tracing copying/forgery and resolving false claims of ownership. However, the negative side is that it may impose overhead on the data/signal/design.

(c) **Public Watermarks:** These types of watermark are insecure as they can be retrieved by anyone through a specific algorithm. However, they are sometimes used to transport intellectual property.

(d) **Private Watermarks:** This type of watermark is secured and can only be retrieved by a secret key.

(e) **Perceptual Watermarks:** This type of watermark is invisible and yet robust. It is based on exploiting limitations of the human sensory systems.

(f) **Bit-stream Watermark:** This type of watermark is used for compressed data such as video.

4. WATERMARKING FOR DOCUMENTS (PAPER, PASSPORT, CURRENCY, AND POSTAL STAMPS)

With the transition of the printing industry to digital platforms, the security of documents has become a major challenge. Digital printing equipment enables users to deploy watermarking in varied environments, but it is a mixed blessing because of the manifold increase in the chances of creation of counterfeit documents. Thus, with better quality and high flexibility of digital platforms, vulnerability to security attacks also increases. Watermarking mechanisms are successfully employed for protection of documents such as paper, bank notes, postal stamps and passports which are all considered immensely valuable in official communications/transactions. In the case of such documents, the inserted watermark is in the form of a picture/image faintly embedded behind the actual text of the document [9, 10, 11]. Some of the properties of such a watermark are as follows:

- The watermark may span the entire document or a certain area of the document.

- The watermark information embedded should, but does not have to, have a relationship with the actual text of the document.
- The watermark should not degrade or obscure the text of the document.
- The watermark must be perceivable by the human eye.
- The watermark must be a recognizable pattern that appears as shades of lightness/darkness when viewed under light transmitted through the document (depending on the thickness of the paper).
- The watermark may be visible by casual inspection or careful examination.
- Authenticity must be recognizable to any user without much complexity.
- Watermarks must not be prone to tampering or changes without disturbing the text.

The process of embedding a watermark in a document can be accomplished in two ways: (a) via the dandy roll process, or (b) via the cylinder mold process. In the first method (shown in Fig.5), a watermark is created by impressing a water coated metal stamp or *dandy roll* onto the paper during the manufacturing process. The dandy roll is a light roller which is covered by a material similar to the one used in a window screen that is imprinted with a pattern, i.e. a mesh like material with a specific design engraved. The still wet reel of paper (pulp) flows under the dandy roll which then imprints by pressure on the paper the designed watermark. The imprint pattern on the dandy roll is typically comprised of a laid wire that runs in parallel to the axis of the dandy roll, and a chain wire that runs around the circumference of the roll. The laid wire imprints light marks on the wet paper while the chain wire produces a strong imprint on the pulp while manufacturing [9, 10, 11].

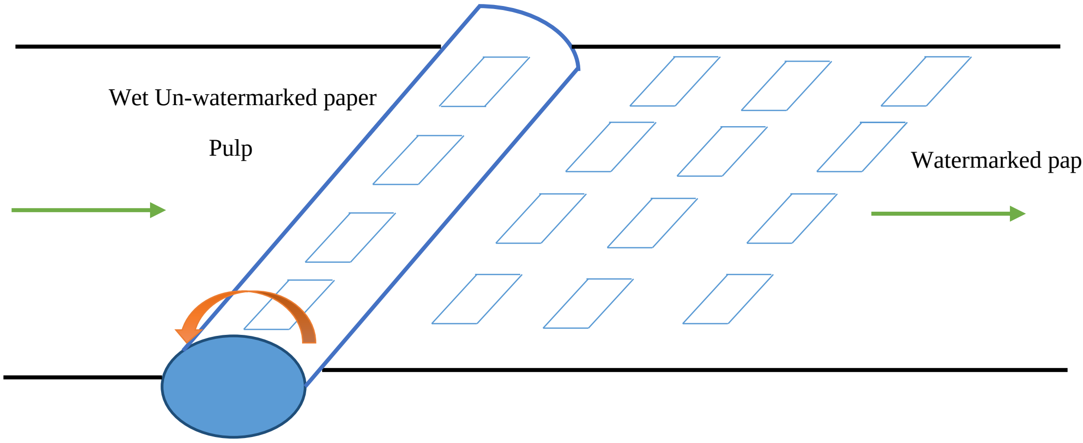


FIGURE 5. Dandy roll watermarking process.

The cylinder mold watermarking method, on the other hand, creates a light to dark shaded imprint resembling a 3D image on the paper. This image is created by areas of relief on the roll itself. This watermarking process is extremely complex, and makes the reproduction of watermarks very challenging, Specifically, the reproduction complexity of watermarks produced by this method is due to the following reasons: (i) the extremely time consuming nature of the process, (ii) the high degree of skill and resources required for watermark creation, and (iii) the requirement of thorough knowledge about the process for creation of watermarks. However, when the costly equipment is available, the process turns out to be simple yet robust. Hence, this process is very frequently used for watermarking of bank notes/currencies, postal stamps and passports to protect the genuine owners/creators from counterfeits/forgery. An example of watermark insertion in bank notes is shown in Fig. 1 [9, 10, 11].

5. DIGITAL WATERMARKING FOR MULTIMEDIA

Digital watermarking of multimedia objects is a process by which data (called ‘watermark’) is embedded into the object such that at a later stage it can be detected or extracted for making an assertion about ownership. A multimedia object can be audio or video clips, images, etc. The generic framework of a watermarking process of multimedia objects comprises of four components: the watermark, the encoder, the decoder and the comparator. There are two components in the watermarking process: i) watermarking insertion algorithm and encoder function, and ii) watermark verification algorithm and decoder function to authenticate the actual owner.

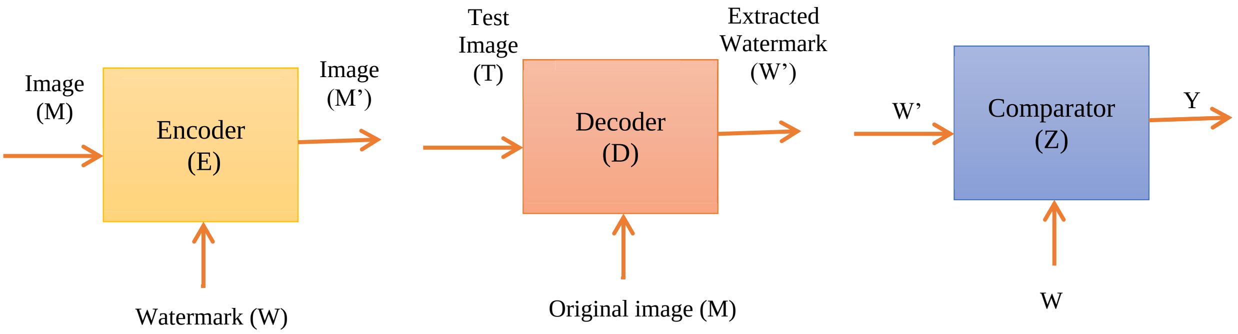


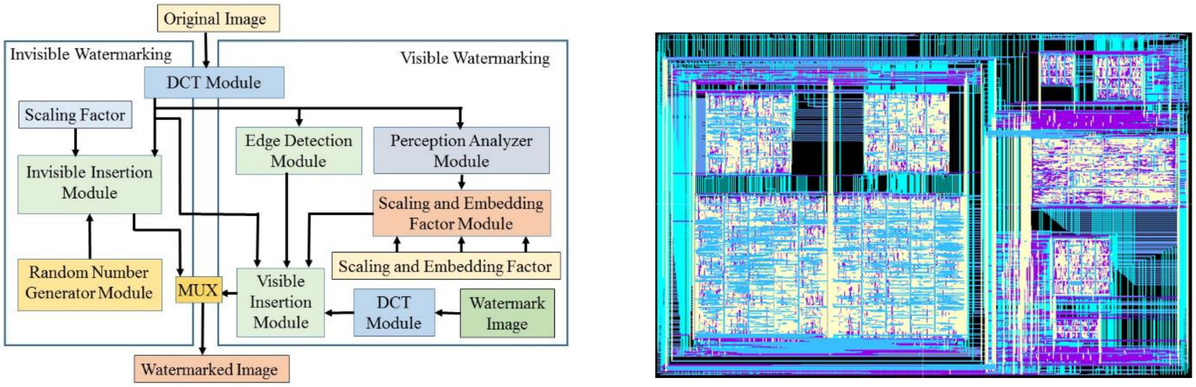
FIGURE 6. Watermarking for multimedia objects

The encoder function (E) accepts an image (M), a watermark (W) and produces as an output a watermarked image (M’). Thus, M’ = E (M, W). The watermark W is dependent on factors such as image size, image feature, identity etc. As a part of a robust watermarking scheme, the decoder function is equally necessary for verification of the actual owner of the multimedia object by resolving claims of ownership in case of conflicts. A decoder functional module could be accomplished in two possible ways: (a) via extraction of the watermark in its original form, or (b) via detection of the watermark location in the original signal/data. Both help in resolving the ownership problem. Thus, the decoder function (D) accepts a test image (T) (*which is either a watermarked image (M’) or a non-watermarked image (M) or a corrupted image (C)*), the original non-watermarked image (M) of (T) and yields as output an extracted watermark image (W’). Thus W’ = D (T, M). The extracted watermark (W’) is compared with the known watermark (W) which is a sequence of digits/bits embedded by the owner, using a comparator function (Z). The output (Y) of the comparator indicates a ‘1’ if there is a match, else yields a ‘0’. Fig. 6 depicts this decoder scheme of digital watermarking [2, 12].

5.1.HARDWARE BASED WATERMARKING SYSTEMS

Hardware based watermarking systems are quite different than software based watermarking schemes. Hardware based watermarking systems can be developed in field programmable gate array (FPGA) emulation platforms, digital signal processor (DSP) boards or application specific integrated circuits (ASIC). Hardware assisted watermarking has also been implemented in graphical processing units (GPU). However, the choice between ASIC, FPGA and GPU is dependent on trade-offs between power, hardware area, speed, and application requirements. Further, the design and implementation of hardware based watermarking solutions are possible for images/videos captured by CMOS image sensors. The watermarking and encoding of an image/video can be integrated into a single system. The watermark system allows adaptation to real stream data with minimum degradation and protection against attacks such as cropping and segment removal from a video sequence, etc. [1].

The datapath architecture and physical design of a watermarking chip are presented Fig. 7 [13, 14]. This watermarking hardware can perform either visible or invisible watermarking depending on the user requirements. The watermarking hardware is an energy-efficient design that can be integrated in any consumer electronics hardware including digital camera, mobile phone, and TV setup box, but will have very minimal energy overhead on them. As shown in Fig.7, modules such as DCT, random number generator and invisible insertion are used for inserting invisible watermarks. The DCT module is used to calculate the DCT coefficients of the host image. Subsequently, the random number is added to them by the insertion module. The modules involved in the visible watermarking are DCT, edge detector responsible for determining the edge blocks of original image, perceptual analyzer, and scaling and embedding module that takes in the visible watermark to be embedded into the watermarked image.



(a) Datapath architecture of an image watermarking chip. (b) Layout of an image watermarking chip.

FIGURE 7. Hardware of chip for digital watermarking [14].

An example of a consumer electronics system with built-in watermarking hardware for images is the secure digital camera (SDC) [15, 16, 17]. Fig. 8 shows a generic system block diagram of a secure digital camera (SDC) with encryption and watermarking units. It comprises of an active pixel sensor unit, a liquid crystal display (LCD), memory, and encryption, compression and watermarking units. In this set-up, an image is captured through the image sensor and is then converted into its digital counterpart through an analog-to-digital converter. The captured image is stored in the memory unit from which it is subsequently displayed in the LCD unit. The image is displayed in the LCD such that the user may see the image before watermarking is applied. Both visible and invisible watermarking algorithms are used along with encryption and compression units for different purpose. The block diagram of the SDC presented here is a generic one; it can be customized to suit the requirements of any specific application.

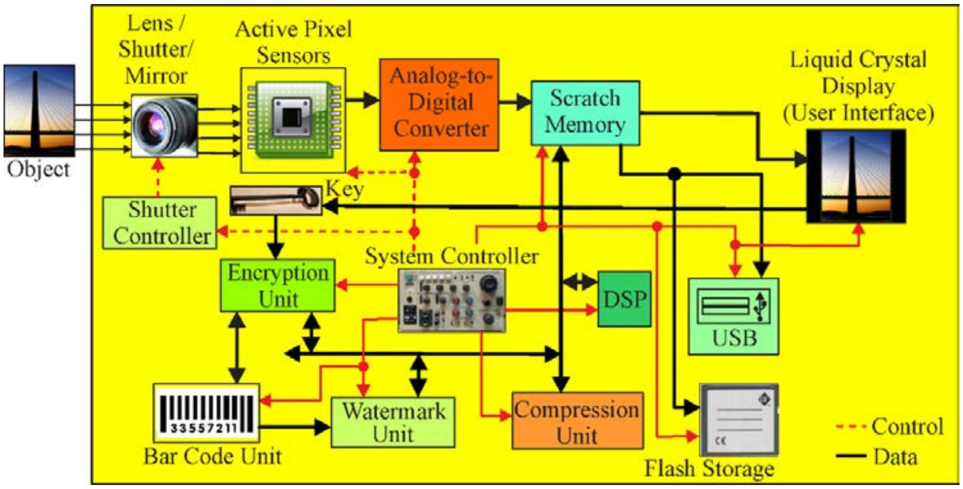


FIGURE 8. Architecture of the Secure Digital Camera (SDC) with built-in capability for real-time Digital Right Management (DRM) [17].

Consumer electronics systems such as digital video recorders and smart phones with video recording capabilities can provide content protected with some form of DRM features if video watermarking hardware is integrated in them [18, 19]. A specific example of a video watermarking hardware architecture is presented in Fig. 9 [19, 20]. The system architecture components include a frame buffer, discrete cosine transformation (DCT), inverse DCT (IDCT), motion estimation (ME), zigzag scanning (ZZ), inverse zigzag scanning (IZZ), entropy coding, inverse entropy coding (IE), quantization, inverse quantization (IQuan), motion compensation (MC), watermarking embedding modules, and the controller. The video stream to be watermarked is not a sequence of independent frames as still images are, but a sequence of correlated frames in the temporal mode, i.e., inter frames (P or B) predicted from the intra frame. So, every object in the base intra frame is inherited by the predicted inter frames (P or B) such that the watermark in intra frames appears in inter frames (P or B) even though they are not embedded with the watermark. However, if it overlaps with any moving objects in the video scene, the watermark drifts around with the moving objects. Drift compensation plays an important role to cancel this side effect and obtain a stable watermark in the compressed video. The motion compensation (MC) module with reference frame and motion vectors, prediction errors, rebuilds a new frame resembling the original one. If it is an intra frame, this block is skipped. The watermark embedding IBP module embeds a watermark to every frame, I, B, P, sequentially; inter frames B and P have two watermarks. One inherited from the intra frame, and one embedded by the component module. The one inherited is the one drifting in inter frames (B and P). The watermark embedding block embeds a watermark to intra frames only.

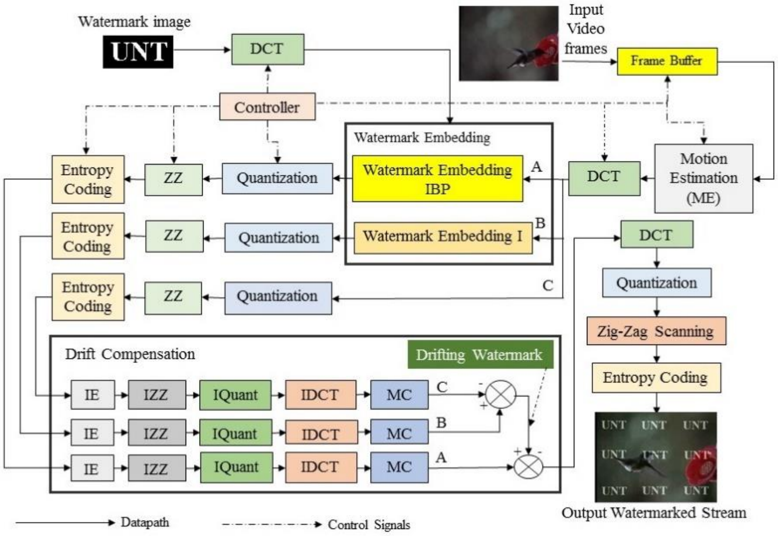


FIGURE 9. System architecture of MPEG video watermarking on compressed domain [20].

Watermarking in the framework of the Better Portable Graphics (BPG) image compression format is being explored to ensure its use in the Internet of Things (IoT) [21]. BPG compression is specifically advantageous for real time and low bandwidth applications due to the low size and high quality images produced which are limitations of the widely used JPEG compression. The interesting characteristics of BPG that differentiate it from JPEG and make it an excellent choice include the following: 1) BPG is open source. 2) high quality and lower size can meet modern display requirements. 3) BPG compression is based on the High Efficiency Video Coding (HEVC), which is a major advance in compression techniques. 4) BPG is supported by most web browsers with a small Javascript decoder. 5) BPG is close in spirit to JPEG and can offer lossless compression in the digital domain. 6) Different chroma formats supported include grayscale, RGB, YCgCo, YCbCr, Non-premultiplied alpha, and Premultiplied alpha. 7) BPG uses a range of metadata for efficient conversion including EXIF, ICC profile, and XMP.

5.2.SOFTWARE BASED WATERMARKING SYSTEMS

Both spatial and frequency domain methods can be used for embedding watermarks, but spatial domain methods are more popular because they are less computationally expensive and easy to implement using software. However, cropping poses a serious threat to any spatial-domain watermarking scheme compared to a frequency domain watermarking method. Hence, in some sophisticated applications, frequency domain methods are used for embedding watermarks. Lossy compression operations that are typically performed in the frequency domain achieve a high level of compression without significant signal degradation by eliminating perceptually non-salient features of the multimedia object. The watermark is inserted in the significant frequency region, i.e. the low frequency components of a multimedia object [1].

6. DIGITAL WATERMARKING FOR CHIP/HARDWARE PROTECTION

Intellectual Property (IP) core/hardware protection is a multi-faceted problem comprising of Trojan security, vendor ownership security, buyer ownership security, transient fault security, security against IP piracy, and fault tolerance [12, 22, 23] Vendor ownership security is a very frequent problem encountered as a part of IP core protection, and is dealt through solutions such as watermarking. Digital watermarking for hardware design protection is an emerging area of research which has gained prominence recently in the CAD/VLSI community. Watermarking has recently been extended to provide protection against false claims of ownership and IP core piracy. Digital watermarking can be embedded in different levels of hardware design abstraction based on the designer's choice, where each level is imposing different trade-off choices and design overhead [24, 25].

For the current generation of hardware design, multi-vendor IP core integration has become a mainstream practice as it helps to achieve maximization of design productivity and minimization of design time. An IP core is a piece of reusable design with many man years of investment. An IP core owner is entitled to legal ownership rights which must be protected against false claims of ownership. Thus, embedding a digital watermark in the form of an encoded message (owner's sequence of digits) in the design is critical from the vendor's perspective. Embedding a watermark in hardware design (regardless of the level of abstraction) must satisfy several desirable properties such as [24, 25]:

- Must not be detectable through normal scan.
- Must not be easily reverse engineered by an adversary who does not have full knowledge of the encoding rules.
- Must be fault-tolerant, i.e. it should have the ability to withstand minor tampering and indicate the rightful owner.
- Must yield minimal design overhead in terms of hardware area and delay.
- Unlike multimedia objects, watermarking for hardware protection must have zero tolerance for design/signal quality degradation.
- Must not even slightly alter the design functionality of the IP core.
- Must have low implementation complexity during embedding as well as reverse engineering for a genuine user.
- Must be robust against standard attacks.
- Must be adaptable to suit modern CAD design tools.

A watermark for an IP core protection is performed by embedding a vendor signature (in the form of encoded digits) in any one or a combination of design steps. One of the specific embodiments of watermarking is deployment for IP protection by embedding vendor signature during high level synthesis (i.e., at higher abstraction layers). The register allocation phase during high level synthesis is a step where the vendor signature can be embedded as extra constraints such that storage variables are forced to execute through distinct registers (based on the encoding rule). However, it should not result in much storage overhead and schedule delay. Multi-variable signature encoding based digital watermarking is considered more robust due to the involvement of more than two encoding variables resulting in difficulty of reverse engineering by an adversary. Embedding the watermark at a higher abstraction level provides flexibility to choose an optimal design candidate solution (through design space exploration) which minimizes the design overhead. Further, the watermark may be embedded in register transfer level (RTL) designs in the form of dummy gates/blocks etc., without disturbing the functionality of the design, as well as at the FPGA level in the form of bitstreams. Moreover, watermarking can be also embedded in the layout file of the design for owner protection. Thus, a robust digital watermark can act as a final line of defense against external threats such as piracy, tampering, false claim of ownership etc. Watermark insertion during any of the design stages of chip design is shown in Fig. 10.

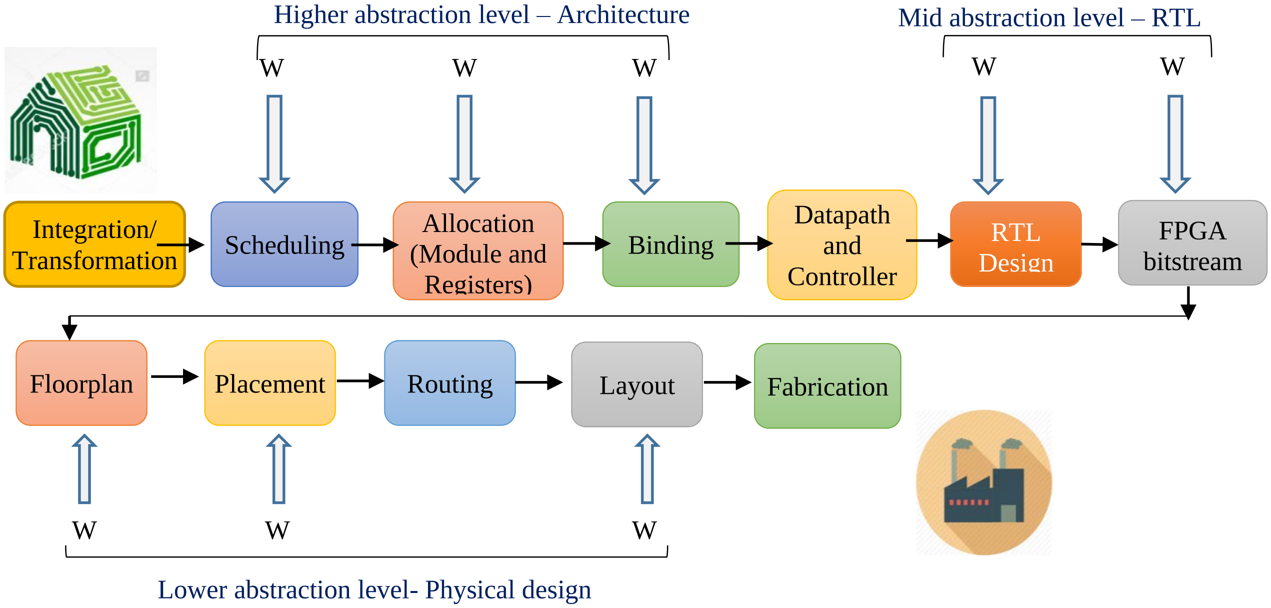

Higher abstraction level – Architecture
Mid abstraction level – RTL
W
W
W
W
W
Integration/ Transformation
Scheduling
Allocation (Module and Registers)
Binding
Datapath and Controller
RTL Design
FPGA bitstream
Floorplan
Placement
Routing
Layout
Fabrication
W
W
W
Lower abstraction level- Physical design

FIGURE 10. Watermark (W) insertion during any of the different stages of Hardware Design.

For the successful resolution of ownership conflict/IP piracy through digital watermarks, signature detection is an essential step. Signature detection comprises of reverse engineering and signature verification. Reverse engineering comprises of collecting structural information of the design and re-generating the design till a certain step (say datapath schematic). Signature verification comprises of decoding the signature to regenerate the additional constraints (watermark). This is followed by verifying the presence of these additional watermarking constraints in the reverse engineered design. An overview is shown in Fig. 11 [25].

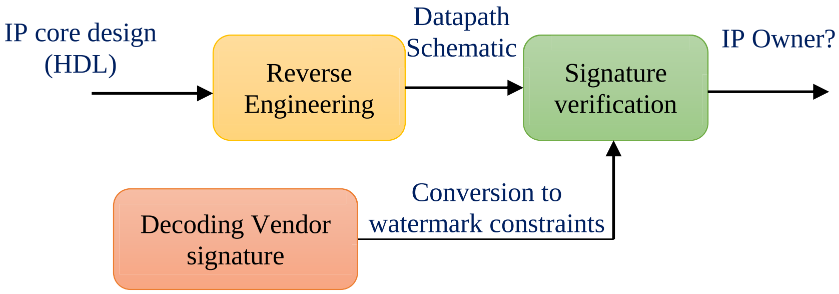


FIGURE 11. Signature detection process for watermarks.

7. SECURITY AND PERFORMANCE METRICS OF DIGITAL WATERMARKING

Some of the popular security and performance metrics used for evaluating a watermarking algorithm are as follows [25]:

(a) **Probability of Co-incidence**: This metric indicates the proof of ownership/authorship, i.e. the strength/quality of a digital watermark. It is measured as the probability of generating the same solution with owner signature. This metric is lower for large values of watermark signature/strong watermark. The larger the size of the signature digits/encoded message, the lower the value of probability of co-incidence will be

(b) **Probability of Tampering:** This metric also indicates the proof of ownership/authorship. It measures the probability of removing one or more signature digits of an encoded message. The probability of tampering increases with the increase in watermark strength (i.e. increase in signature digits/encoded message sequence).

(c) **Embedding Cost:** Probability of co-incidence and probability of tampering are orthogonal in nature. This is because to have a desirable low probability of co-incidence, a large size watermark is required; however, that increases the probability of tampering which is undesirable. Thus, there needs to be a tradeoff. Further, increase in watermark strength although it makes the data/signal/design robust (which is desirable), concurrently also increases the likelihood of overhead/degradation of quality (which is undesirable). Thus, there needs to be a tradeoff again in this case.

(d) **Watermark Embedding Time and Watermark Detection Time:** The complexity of adding the watermark should not yield a high time complexity/runtime overhead. It should be seamlessly adaptable to the data without disturbing its content. Similarly, the watermark detection time should be very low such that for a knowledgeable entity decoding and verifying the signature should be smooth.

8. CONCLUSIONS

An all-inclusive view of watermarking is described in this paper including its background, motivation, classification techniques as well as various relevant applications. This paper presented a holistic view of watermarks used in various applications of our everyday life ranging from paper marks, currency/postal stamps, multimedia, to hardware protection. Further, desirable watermarking properties, a comparative analysis of regular and digital watermarks, and security metrics (such as probability of co-incidence and probability of tampering) were discussed. The paper provides an insight into watermarking approaches used in real life today. More explicitly, it emphasizes the deep relevance of watermarking in various domains ranging from mechanical, electrical to computer engineering applications. The future evolution of watermarking lies in improving robustness, overhead, runtime complexity and security models for quality evaluation. Watermarking usage for verification of data trustworthiness can be important for emerging IoT and bigdata frameworks [22]. Watermarking integrated in the sensor nodes for critical applications to ensure that the data received at remote ends is trustworthy is one of the emerging applications [26].

ABOUT THE AUTHORS

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the Department of Computer Science and Engineering, University of North Texas. He is an inventor of 4 US patents. He is an author of 220 peer-reviewed research articles and 3 books. He is currently the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine. He currently serves on the editorial board of 6 peer-reviewed international journals including IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems and ACM Journal on Emerging Technologies in Computing Systems. Prof. Mohanty has been the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) to oversee a dozen of IEEE conferences. He serves on the steering, organizing, and program committees of several international conferences. More about him can be available from: http://www.smohanty.org.

Anirban Sengupta (asengupt@iiti.ac.in) is an Assistant Professor in Computer Science and Engineering at Indian Institute of Technology Indore, where he directs the research lab on 'Behavioural Synthesis of Digital IP core. His research projects are funded & supported by government agencies and industries. He is an author/inventor of more than 100 Publications & Patents and Honorary Chief Scientist at VividSparks IT Solutions Pvt Ltd. He currently serves in Editorial positions of 8 IEEE, Elsevier, & IET Journals as Editor, Executive Editor, Associate Editor, Columnist and Guest Editor. He serves as Guest Editor of IEEE Transactions on VLSI Systems, IEEE Transactions on Consumer Electronics and IEEE Access Journals. He is further serving as Editor of Elsevier Microelectronics Journal, Associate Editor of IET Computer & Digital Techniques, Executive Editor & Columnist of IEEE Consumer Electronics Magazine, Associate Editor of IEEE VLSI Circuits & Systems Letter (VCAL) and Associate Editor of IEEE Access Journal. More about him can be available from: http://www.iiti.ac.in/~asengupt.

Parthasarathy Guturu (Parthasarathy.Guturu@unt.edu) is an Associate Professor in Electrical Engineering at the University of North Texas. He obtained a Ph.D. (Engineering) in Pattern Recognition- all from Indian Institute of Technology, Kharagpur. He published over 50 papers in international journals and conferences in the areas of Pattern Recognition, Computer Vision/Image Processing, Artificial Intelligence, and Neural Networks/Genetic Algorithms. He contributed to the areas of Intelligent Networks and 3G Wireless Systems and holds 3 patents.

Elias Kougianos (eliask@unt.edu) is Professor in Electrical Engineering Technology at the University of North Texas. He obtained his Ph.D. in electrical engineering from Louisiana State University in 1997. He is author or co-author of over 100 peer-reviewed journal and conference publications. He is a Senior Member of IEEE.

REFERENCES

[1] S. P. Mohanty, "ISWAR: An Imaging System with Watermarking and Attack Resilience", *The Computing Research Repository (CoRR), ArXiv e-prints*, 1205.4489, May 2012, 21-pages.

[2] G. Voyatzis, Ioannis Pitas "The Use of Watermarks in the Protection of Digital Multimedia Products", *Proceedings of the IEEE*, Vol. 87, No. 7, July 1999, pp. 1197 – 1207.

[3] Peter Corcoran and Claudia Costache, "Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts", *IEEE Consumer Electronics Magazine*, Volume: 5, Issue: 2, pp. 70 – 78, 2016.

[4] Jeff Yurek Ultra "High Definition: Beyond pixel count", *IEEE Consumer Electronics Magazine*, Volume: 4, Issue: 4, pp. 89 - 91, 2015.

[5] C. H. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, *1st Ed.: Idea Group Publishing*, 2005.

[6] Ingemar J. Cox, Gwenaël Doërr, Teddy Furon, "Watermarking Is Not Cryptography", *Lecture Notes in Computer Science, Springer*, Volume 4283, 2006, pp 1-15.

[7] B. Norris and M. Humphries, Digital Rights Management, http://www.drm.web.unc.edu/what-is-drm/, Accessed on Oct 2016.

[8] R. Chandramouli, Nasir Memon, Majid Rabbani "Digital Watermarking", *Encyclopedia of Imaging Science and Technology*, JAN 2002, DOI: 10.1002/0471443395.img010.

[9] J. C. Biermann, Handbook of Pulping and Papermaking (2ed.), San Diego, California, USA: *Academic Press*., ISBN 0-12-097362-6, 1996.

[10] Johnson Dandy, Dandy Roll, http://www.johnstondandy.com/dandyrolls.html, Accessed on September 2016.

[11] Kin-ya Hiyoshi, Takayuki Fukuchi, Tadahiro Iwasaki, "Method of producing watermark paper", *US Patent* 5766416A, 1998.

[12] S. P. Mohanty, Nanoelectronic Mixed-Signal System Design, McGraw-Hill, 2015, ISBN-10: 0071825711, ISBN-13: 978-0071825719.

[13] E. Kougianos, S. P. Mohanty, and R. N. Mahapatra, "Hardware Assisted Watermarking for Multimedia", *Elsevier International Journal on Computers and Electrical Engineering*, Volume 35, Issue 2, March, 2009, pp. 339-358.

[14] S. P. Mohanty, N. Ranganathan, and K. Balakrishnan, "A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain", *IEEE Transactions on Circuits and Systems II (TCAS-II)*, Vol. 53, No. 5, May 2006, pp. 394-398.

[15] S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", *Elsevier Journal of Systems Architecture*, Volume 55, Issues 10-12, December 2009, pp. 468-480.

[16] Thomas Winkler, Adam Erdelyi, and Bernhard Rinner, "TrustEYE M4: Protecting the Sensor--not the Camera", in *Proceedings of the International Conference on Advanced Video and Signal Based Surveillance*, 2014.

[17] O. B. Adamo, S. P. Mohanty, E. Kougianos, and M. Varanasi, "VLSI Architecture for Encryption and Watermarking Units Towards the Making of a Secure Digital Camera", in *Proceedings of the IEEE International SOC Conference (SOCC)*, pp. 141-144, 2006.

[18] S. D. Roy, X. Li, Y. Shoshan, A. Fish, and O. Yadid-Pecht, "Hardware Implementation of a Digital Watermarking System for Video Authentication", *IEEE Transactions on Circuits and Systems for Video Technology*, 23 (2): 289–301, 2013.

[19] S. P. Mohanty and E. Kougianos, "Real-Time Perceptual Watermarking Architectures for Video Broadcasting", *Elsevier Journal of Systems and Software (JSS)*, Vol. 84, No. 5, May 2011, pp. 724--738.

[20] S. P. Mohanty, E. Kougianos, Wei Cai, and M. Ratnani, "VLSI Architectures of Perceptual Based Video Watermarking for Real-Time Copyright Protection", in *Proceedings of the 10th International Symposium on Quality Electronic Design (ISQED)*, pp. 527-534, 2009.

[21] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things (Invited Paper)", *IEEE Access Journal*, Volume 4, 2016, pp. 1222--1242.

[22] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 6, Issue 3, July 2016, pp. 60--70.

[23] A. Sengupta, S. Bhadauria, and S. P. Mohanty, “TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor during High Level Synthesis”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, Volume 99, Issue 99, 2016, pp. Accepted on 24 July 2016.

[24] A. Sengupta, S. Bhadauria, “IP core Protection of CDFGs using Robust Watermarking during Behavioral Synthesis Based on User Resource Constraint and Loop Unrolling Factor”, *IET Electronics Letters*, Vol. 52 No. 6 pp. 439-441, March 2016.

[25] A. Sengupta, S. Bhadauria, “Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis”, *IEEE Access Journal*, Volume:4, Issue: 99, pp. 2198 - 2215, May 2016.

[26] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and U. Choppali, “Wireless Sensor Network Simulation Frameworks: A Tutorial Review”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 6, Issue 2, April 2016, pp. 63--69.