Lossless Watermarking for Image Authentication: A New Framework and an Implementation

Mehmet Utku Celik, *Member, IEEE*, Gaurav Sharma, *Senior Member, IEEE*, and A. Murat Tekalp, *Fellow, IEEE*

***Abstract*—We present a novel framework for lossless (invertible) authentication watermarking, which enables zero-distortion reconstruction of the un-watermarked images upon verification. As opposed to earlier lossless authentication methods that required reconstruction of the original image prior to validation, the new framework allows validation of the watermarked images before recovery of the original image. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. For verified images, integrity of the reconstructed image is ensured by the uniqueness of the reconstruction procedure. The framework also enables public(-key) authentication without granting access to the perfect original and allows for efficient tamper localization. Effectiveness of the framework is demonstrated by implementing the framework using hierarchical image authentication along with lossless generalized-least significant bit data embedding.**

***Index Terms*—Forgery detection, invertible authentication, lossless compression, reversible data embedding, tamper localization.**

I. Introduction

TRADITIONALLY, source authentication and integrity verification of digital data have been performed by *digital signatures*. A digital signature is a data string which associates (binds) a piece of information (in digital form) with some originating entity [2], [3]. With the availability of sophisticated image/video editing tools, authentication of multimedia data is gaining importance. Image authentication in traditional manner requires the storage and transmission of signature strings in the image header [4]. This method imposes limitations on the image/file format—sometimes preventing implementation in legacy systems. It is also susceptible to loss during format conversions—even if the underlying image data remains intact. It is therefore desirable to include the digital signatures within the image data. This goal can be achieved using watermarks [5]–[8], which exploit the redundancy in the image data and the insensitivity of the human visual system (HVS) to small distortions. In addition to format independence, digital watermarks have the advantage of *tamper localization*, which refers to the ability to identify the image regions that have been tampered (manipulated) after insertion of the watermark.

The functionality offered by digital watermarks, however, often comes at the expense of image fidelity. Most watermarking techniques modify, and hence distort, the host signal in order to insert authentication information. In many applications, loss of image fidelity is not prohibitive as long as original and modified images are perceptually equivalent. On the other hand, in medical, military, and legal imaging applications, where the need for authentication is often paramount, there are typically stringent constraints on data fidelity that prohibit any permanent signal distortion in the watermarking process.

The loss of signal fidelity can be remedied by the use of *lossless* (also referred as *reversible*, *invertible*, or *distortion-free*) authentication watermarks[1] [9]–[11]. These methods, like their lossy counterparts, insert authentication information by modifying the host signal, thus induce an embedding distortion. Nevertheless, they also enable the removal of such distortions and hence exact—lossless—restoration of the original host signal.

The original contribution of this paper is a novel lossless authentication framework. As opposed to earlier schemes, this framework validates the authenticity and integrity of watermarked images *before* attempting to reconstruct the original image. If the verification step is successful, the integrity of the reconstructed (original) image is inferred from the uniqueness of the reconstruction procedure. This reduces computational requirements in situations when either the verification step fails or the zero-distortion reconstruction is not needed. The framework also enables public(-key) authentication without granting access to the perfect original and allows for efficient tamper localization.

In Sections II and III, we present a brief overview of existing methods and the proposed framework, respectively. A specific implementation of the framework and related experimental results are discussed in Section IV. Conclusions are drawn in Section V.

II. Background

A generalized block diagram that is representative of the prior lossless authentication watermarking schemes is seen in Fig. 1. In these methods, the watermark embedding phase has two stages: *a*) an authentication-information (e.g., digital signature) computation step; and *b*) a lossless (reversible) data embedding step, in which the computed information is inserted

Manuscript received August 10, 2004; revised April 12, 2005. This work was presented in part at the 2003 Electronic Imaging Symposium [1]. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Benoit Macq.

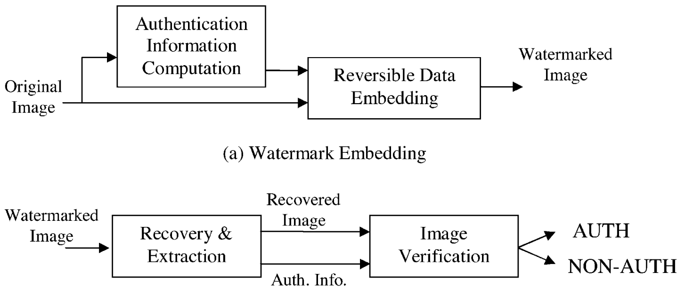
M. U. Celik was with the University of Rochester, Rochester, NY 14627-0126 USA. He is now with is with the Information and Systems Security Department, Philips Research, Eindhoven, 5656 AA, The Netherlands (e-mail: u.celik@ieee.org.).

G. Sharma is with the Electrical and Computer Engineering Department, University of Rochester, Rochester, NY 14627-0126 USA (e-mail: gaurav.sharma@rochester.edu; g.sharma@ieee.org).

A. M. Tekalp is with the Electrical and Computer Engineering Department, University of Rochester, Rochester, NY 14627-0126 USA, and also with the College of Engineering, Koc University, Istanbul, Turkey (e-mail: tekalp@ece.rochester.edu; mtekalp@ku.edu.tr).

Digital Object Identifier 10.1109/TIP.2005.863053

[1] In this paper, we limit our scope to *fragile* authentication watermarks, which provide exact, i.e., bit per bit, integrity verification. Earlier lossless authentication watermarks have also been of this type.



(a) Watermark Embedding

(b) Image Recovery and Verification

Fig. 1. Prior lossless authentication watermarking schemes. (a) Watermark embedding and (b) image recovery and verification.

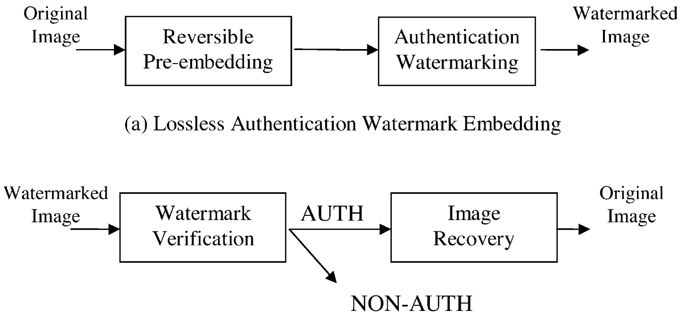
into the image data in a reversible manner. During the recovery and verification phase, first the data embedding process is reversed to yield an estimate for the original image and the authentication information. If the watermarked image has not been altered, the extracted information validates the estimated image and this estimate is labeled as an authentic original.

Virtually all existing schemes [9]–[14] follow this framework with differences in the lossless data embedding step. In [9], Fridrich *et al.* implemented the lossless data embedding step by compression and replacement of one or more least-significant bit planes of the image data. Later, the authors proposed a more efficient algorithm based on RS-embedding method [13]. Meanwhile, Honsinger *et al.* [10] proposed using a spread-spectrum watermark with modulo-addition for lossless reconstruction. Similarly, De Vleeschouwer *et al.*, Tian and van der Veen have proposed methods based on the circular interpretation of the image histogram [14], difference expansion [11], and histogram modifications [15], respectively.

In [16], Dittmann *et al.* proposed an alternative protocol based on the least significant bit (LSB) compression technique of [9]. The protocol utilizes a public and a private key signature corresponding to the most and least significant bit planes, respectively. When combined with the encryption of the compressed LSB information, the method allows for public-key verification of the watermarked image while reserving the reconstruction of the perfect original to the authorized parties that hold the private-key. Despite the added functionality, the protocol is not extensible to all lossless embedding methods, for instance Honsinger's method [10]. Furthermore, it requires an increased payload, thus a higher embedding distortion, due to the second signature. Note that none of the lossless authentication methods in the literature offer tamper localization capability, which is one of the major advantages of authentication watermarks over conventional digital signatures.

III. New Lossless Authentication Watermarking Framework: LAW

A generalized framework that encompasses existing lossless authentication watermarks was presented in the preceding section. Here, we propose a new framework that we refer to as lossless authentication watermarking *LAW*. LAW enhances the functionality and reduces the complexity of earlier methods. A specific implementation of the LAW framework is discussed in the next section.



(a) Lossless Authentication Watermark Embedding

(b) Watermark Verification and Recovery

Fig. 2. New lossless authentication watermarking framework: *LAW*. (a) Lossless authentication watermark embedding and (b) watermark verification and recovery.

LAW achieves its performance advantages over the existing framework by *interchanging the order of the authentication information computation and reversible embedding steps*. Fig. 2 is a high-level block diagram of LAW that shows the watermark embedding and verification phases. The watermark embedding phase comprises of two steps: a) lossless (reversible) pre-embedding and b) (nonreversible) authentication watermarking. The actions of these two steps are coordinated together by partitioning the code space used for storage of image data into two disjoint parts, P_A and P_I, which together comprise the complete code space. For example, the code space may use a subset of LSBs for P_A and the remaining bits for P_I. In other schemes, such as [11], P_A and P_I may be partitions of wavelet coefficient space. In the watermarked image, the part P_A carries authentication information and the part P_I carries (complete) original image information. In the pre-embedding step, original image data in P_A is reversibly embedded into the data in P_I. Next, in the authentication watermarking step, authentication information for data in P_I (which has been modified in a reversible manner in the preceding step) is computed and placed in part P_A. Note that the placement of data in P_A does not alter the data in P_I. The reversibility of the pre-embedding thus ensures that the full image data is recoverable from data in partition P_I in the watermarked image.

The verification phase of LAW, which is run at the receiver side, is shown in Fig. 2(b) and comprises of two steps: a) authentication watermark verification, and if the verification step is successful, b) original image recovery. Note that in conformance with the altered ordering at the embedder, the order of these two steps is interchanged, at the receiver too, in relation to the earlier framework of Fig. 1. In the first step, authentication information is extracted from part P_A and is used to validate the integrity of data in part P_I. If a third party has tampered with the image data after the watermark insertion, the extracted authentication information does not match the image data and image is deemed nonauthentic. Otherwise, the watermarked image is considered authentic, i.e., unaltered since the watermark insertion. In the latter case, original image may be reconstructed from the data in part P_I by reversing the lossless data embedding step and restoring the part P_A of the image that is modified by the authentication watermark. Note that, upon successful verification, integrity of the final reconstructed image is ensured by the uniqueness of the reconstruction process.

Advantages of the LAW Framework: The reversal in the order of authentication and lossless watermarking steps (with respect to earlier methods [9]–[14]) results in reduced computational burden and additional functionality, described as follows.

- *Computational advantages in the verification phase.*

  As opposed to earlier methods, the LAW framework validates the images *before* attempting to reconstruct the original image. As a result, the image reconstruction step may be skipped when either *a*) the verification step fails, or *b*) the watermarked image meets the quality criteria and the perfect original is not needed. The computational savings are often substantial due to the complexity of the reconstruction step.
- *Computational advantages in the embedding phase.*

  In client/server applications where a single image is served to multiple clients with different signatures (or time-stamps), the LAW framework has additional computational advantages. In this case, the server performs the—often costly—pre-embedding step only once and inserts different signatures as requested by clients.
- *Public/private-key support.*

  The LAW framework also supports the public-validation/private-recovery property of [16], without the need for a second signature. When a public-key authentication signature is used in conjunction with a private-key dependent lossless watermark, the framework supports public validation of the watermarked image, but limits access to the perfect original.
- *Accurate tamper localization.*

  Another advantage of the new framework is the ability to support efficient and accurate tamper localization. Most (nonreversible) authentication watermarks (e.g., [13], [17]–[19]) offer the ability to pin-point the image regions that have been tampered. This often involves performing the integrity verification on per block basis, where block dimensions determine the localization accuracy. Existing lossless authentication watermarks may provide the same functionality in a similar manner. Nevertheless, lossless data embedding methods used in those schemes are not as efficient when applied on small image blocks.[2] As a result, accurate tamper localization (using small image blocks) has not been feasible with the existing lossless authentication watermarks. In the LAW framework, lossless data embedding (pre-embedding) algorithm processes the whole image in a single step with high efficiency. The resultant capacity is then shared between small blocks for authentication watermarking.
- *Implementation flexibility.*

  The LAW framework may be implemented using different lossless data embedding and authentication watermarking algorithms, as long as the necessary coordination between two steps is established. For instance, a wavelet based reversible embedding scheme [11] may be followed by a spatial domain LSB authentication watermark [17].

In the following section, we provide one proof-of-concept implementation to demonstrate these advantages. As mentioned earlier, several other implementations are also feasible within this framework.

IV. Localized Lossless Authentication Watermark (*L-LAW*)

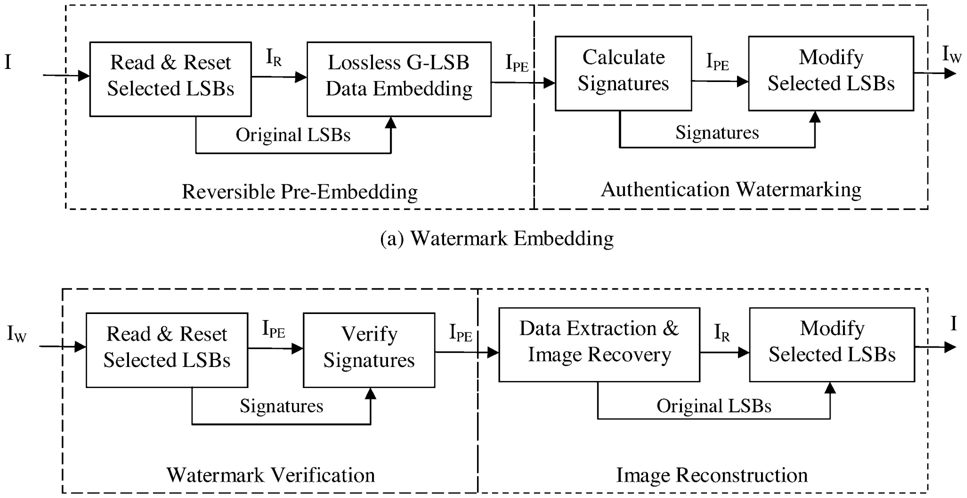
A. Implementation

Localized Lossless Authentication Watermark (L-LAW) is a secure, flexible, computationally efficient lossless image authentication watermark with tamper localization ability, low embedding distortion (which can be removed entirely if necessary) and public/private key support. L-LAW is an implementation of the LAW framework proposed in Section III using the hierarchical image authentication scheme [18] and the lossless generalized-LSB data embedding method [20]. A block diagram detailing the embedding and verification phases of *Localized-LAW* is seen in Fig. 3.

Embedding Phase: As indicated in the preceding section, the watermark embedding phase consists of two steps: *(a)* reversible pre-embedding, and *(b)* authentication watermarking, which are coordinated through suitable partitioning of the image data (storage) locations. Fig. 4 illustrates the particular partitioning for our implementation. The image is divided into blocks that correspond to the elementary localization units of the hierarchical authentication watermark used in the subsequent authentication watermarking step. In each block, LSBs of the first N pixels (in the raster-scan order) are designated to carry the authentication payload, where N and the block sizes are determined by the (cryptographic) security and localization requirements. These selected LSBs constitute the part P_A and in the schematic illustration of Fig. 4 correspond to the LSBs for shaded regions (the nonwhite regions with different shades of gray). The more significant bits (MSBs) for the shaded regions and all the bits for other pixels (shown as white regions in Fig. 4) constitute the part P_I that carries the (complete) image information. Note that the MSBs are defined to include all bits other than the LSBs included in part P_A.

In the pre-embedding step *(a)* of the watermark embedding phase, the LSB values in part P_A (LSBs for dark regions in Fig. 4) are read and reversibly embedded into the rest of the image (white regions in Fig. 4) using *Lossless generalized-LSB (LGLSB) data embedding* [20]. The LGLSB data embedding method creates capacity for lossless insertion of payload data by compressing pixel LSBs, exploiting more-significant-bits (MSBs) as side information for improving compression efficiency. Fig. 5 shows an overview of the method, additional details may be found in [20]. In the embedded version of the image, the LSBs carry the compressed bit stream of original LSBs as well as the payload data. The algorithm may be applied selectively on part of the image, a fact that we exploit in our implementation of pre-embedding: we use the image data in part P_A as the "payload" and embed it in spatial pixel locations corresponding to the white regions shown in Fig. 4. The data in

[2] For instance, compression based lossless data embedding methods typically utilize adaptive compression techniques that gradually "learn" specific image statistics and become efficient. This efficiency can be seriously hampered if one attempts to compress small regions of images independently.



(a) Watermark Embedding

(b) Watermark Verification and Recovery

Fig. 3. Block diagram for *Localized-LAW* method. (A specific instance of the proposed LAW framework.) (a) Watermark embedding and (b) watermark verification and recovery.

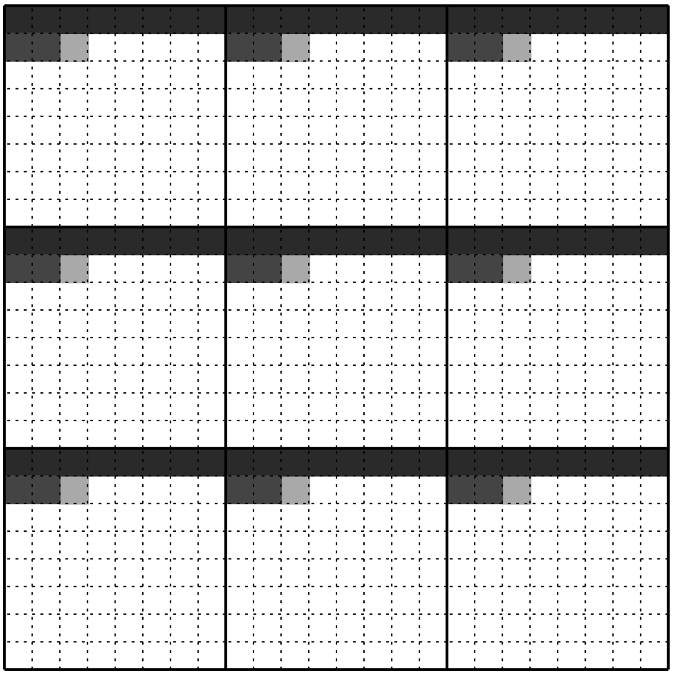


Fig. 4. Image data location (bit) partitioning *L-LAW*. Dotted lines are pixel boundaries. Thick lines form the blocks, which are tamper localization units of the authentication watermark. In each block, LSBs of shaded areas (nonwhite pixels) carry authentication information (forming part P_A). All remaining bits in the image carry image information forming part P_I. Unshaded areas are modified during the pre-embedding step to allow lossless recovery (original LSB values in the dark regions are inserted into these white regions by the lossless G-LSB algorithm).

part P_A, i.e., LSBs in shaded regions of Fig. 4, is then reset to 0 to produce the pre-embedded image.[3]

Note that for better efficiency, lossless data embedding is performed on the image as a whole rather than on a block by block

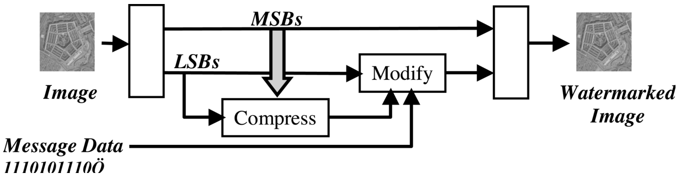


Fig. 5. Lossless generalized-LSB algorithm.

basis. Also observe that encryption of the payload and the compressed bit stream readily yields an implementation in which the recovery of the original image and embedded data is dependent on a cryptographic key.

The authentication watermarking step (b), uses *the hierarchical image authentication scheme* [18] on the image obtained after the pre-embedding step. The hierarchical block-based watermarking technique inserts and extracts a watermark in a multilevel hierarchy. The (nonoverlapping) blocks of the pre-embedded image shown in Fig. 4 constitute the lowest level of the hierarchy. Successive levels of the hierarchy are formed by combining distinct groups of blocks at a preceding level of the hierarchy. In general, the number of blocks from a lower level of the hierarchy that are combined to form a block at the next level of the hierarchy may be arbitrarily chosen, however, in order to keep the notation and the description simpler, we assume for the rest of this paper that the region of 2 × 2 blocks at a given level of the hierarchy are combined to create a block at the next level of the hierarchy, giving us a quad-tree for the hierarchy as shown in Fig. 6.

For each block at each level of the multilevel hierarchy, a digital signature or message authentication code (MAC [2]) is computed for the data (in the pre-embedded image) within the block. A standard digital signature algorithm operates on the concatenation of all binary digits representing the pixel values in the block (blocks at higher level of the hierarchy use all the image bits within the corresponding region). These signature are then placed in the part P_A of the image data locations corresponding to LSBs of shaded regions in Fig. 4. In order to incorporate localization capability, the distribution of the signature information bits also follows the quad-tree hierarchy as illustrated in

[3] The zeroing of selected LSBs is used here to simplify subsequent description. Other values may be used in practice, including key dependent pseudorandom values that may improve cryptanalytic performance. Also note that this is equivalent though slightly different from the LAW framework description in Section III where it was assumed the bits in P_A are excluded in the subsequent authentication watermark.

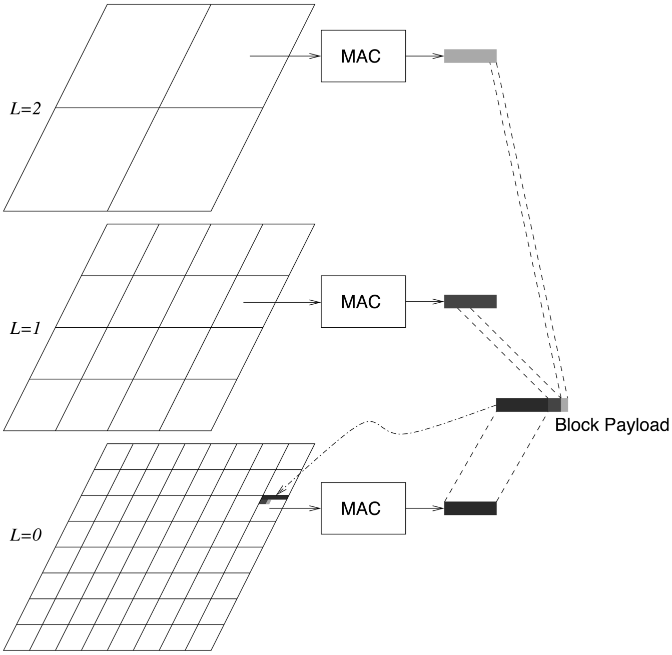


Fig. 6. Organization of block hierarchy and signatures in *L-LAW*. $L = 0$ denotes the lowest level of the hierarchy where the lines depict boundaries of the blocks that form the fundamental localization unit (same as block boundaries in Fig. 4). Blocks at higher levels are composed of four blocks from the preceding level forming a quad-tree. For each block in the hierarchy, a message authentication code (MAC)/digital signature is computed. Authentication information payload for a block is the concatenation of parts of MACs computed at different levels of the hierarchy: all of the $L = 0$ MAC bits, 1/4 of the MAC bits at $L = 1$, and 1/16 of the MAC bits at level $L = 2$. Authentication payload is embedded in part P_A of image bits corresponding to LSBs of shaded regions.

Fig. 6: the LSBs for the shaded region within each block contain all of the signature for the block at the lowest level of the hierarchy in which it is located, 1/4 of the signature bits for the second level of the hierarchy, 1/16 of the signature bits for the third level of the hierarchy, and so on. This packetization of signatures ensures that the signature of each block is contained within the P_A part of image bits for the block. The hierarchical nature of the scheme provides security against vector-quantization attacks [21] and good tamper localization accuracy. Additional details on the hierarchical authentication method may be found in [18].

Verification Phase: On the receiver side, the watermark verification and recovery are performed as illustrated in Fig. 3(b). The process begins by overlaying the grid of image blocks (at the lowest level of the hierarchy) over the image pixels which allows the determination of the parts P_A and P_I that carry authentication information and image information, respectively (as seen in Fig. 4). The (presumed) authentication information from bits constituting part P_A (the LSBs corresponding to shaded regions in Fig. 4) is then extracted and these bits are reset to zero in the image. If the received image is exactly the watermarked image (no alterations), this process recovers the pre-embedded image that was produced at the embedder.

Next, the quad-tree hierarchy of Fig. 6 is overlaid on the image blocks (and the corresponding extracted authentication information) to compute signatures corresponding to each of blocks in the hierarchy and validate these against the signatures already extracted from part P_A. First, the signature for the entire image (corresponding to the highest level of the hierarchy) is computed and verified against the signature computed from the (presumed) pre-embedded image already recovered. If the image/signature pair is valid, the image is deemed authentic and (if required) the recovery component of the lossless G-LSB algorithm is utilized to extract and restore the original LSBs, effectively reconstructing the original image. If the image signature verification step fails, the hierarchical authentication scheme determines the tampered regions. That is, for each level of the hierarchy, it computes the block signatures and validates these against the corresponding signatures that were extracted from part P_A and recovered using the hierarchical quad-tree. Invalid blocks are indicated on a tamper localization map, as seen in Fig. 9. For each region, the method indicates the highest level of the authentication hierarchy for which the embedded signature is valid. Additional details of the verification process may be found in [18].

B. Experimental Results

For the results discussed in this section, we chose the following parameters in our *L-LAW* implementation.

- *Image signature:* A public-key digital signature is computed from the whole image. Specs: 320-bit DSA with a 1024-bit key (see [2]).
- *Block signature:* A private(secret)-key message authentication code is computed for each block. Specs: 64-bit HMAC derived from MD5 with a 128-bit key (see [2]).
- *Block hierarchy:* Minimum block size is chosen as 64 × 64 pixels. At each successive level of the hierarchy block size is quadrupled (e.g., 256 × 256, 1024 × 1024, ...). This provides sufficient tamper localization accuracy (64 × 64) with a small payload requirement.
- *Pre-embedding level:* Parameters of the lossless G-LSB modification method [20] used in the reversible pre-embedding step are determined automatically to accommodate the resulting payload.
- *Pre-embedding key:* In the lossless G-LSB embedding method [20], the compressed bit stream is encrypted using the AES [2] algorithm with a 128-bit key.

A 1024 × 1024 grayscale image is watermarked using *Localized-LAW* algorithm. The watermarked image (Fig. 7) is visually identical to the original (not shown) at a peak-signal-to-noise-ratio (PSNR) of 50.85 dB [PSNR is defined as $\mathrm{PSNR} = 10\log_{10}(255^2/\mathrm{MSE})$].

In the absence of further manipulations, a) with knowledge of the public key (corresponding to the key pair used for the image signature), the integrity of the whole image may be verified; b) with knowledge of the AES key used in the pre-embedding, the mathematically lossless original may be recovered from the watermarked image.

In the presence of manipulations, the public key based image authentication indicates a compromise of the image integrity and the private key based block signatures allow localization of the manipulations. We illustrate this by means of an example. In order to simulate a malicious attacker, the watermarked image has been altered using an off-the-shelf image manipulation program. In particular, vehicles around the structure at the center

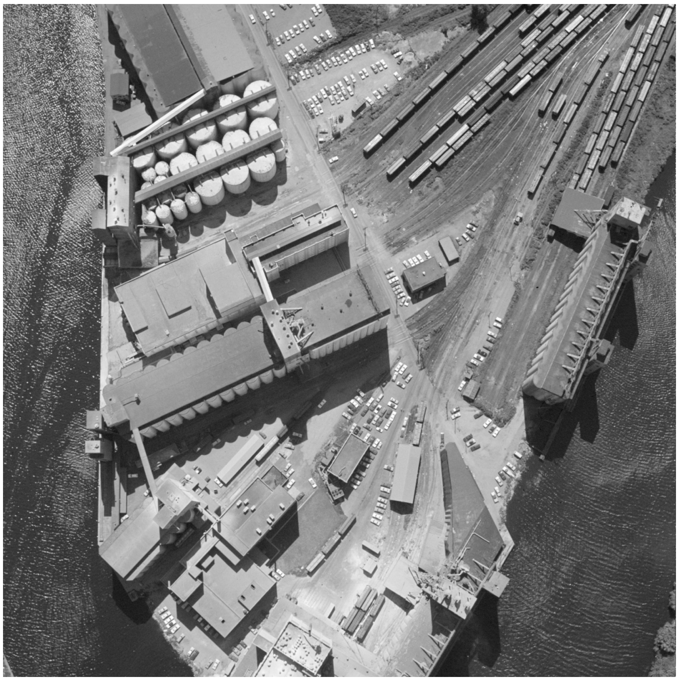


Fig. 7. Watermarked image. PSNR 50.85 dB.

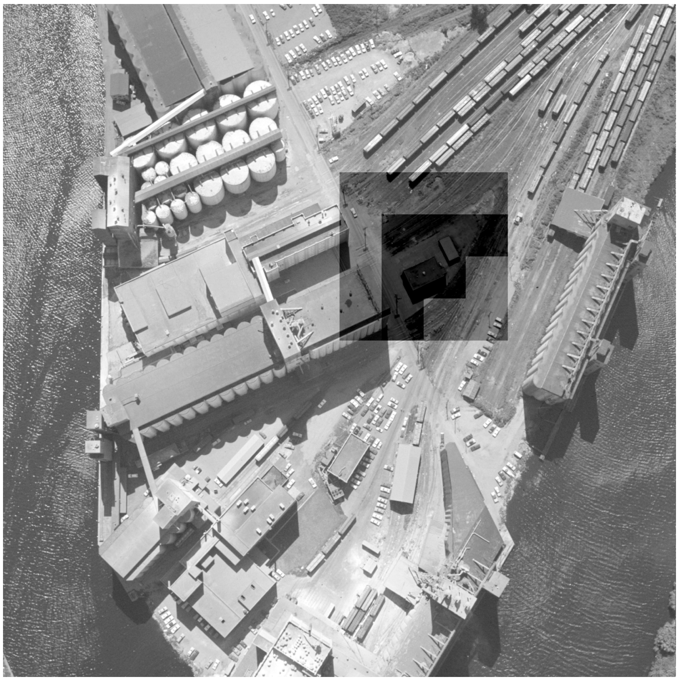


Fig. 9. Watermark detection output. Dark regions signal image manipulation.

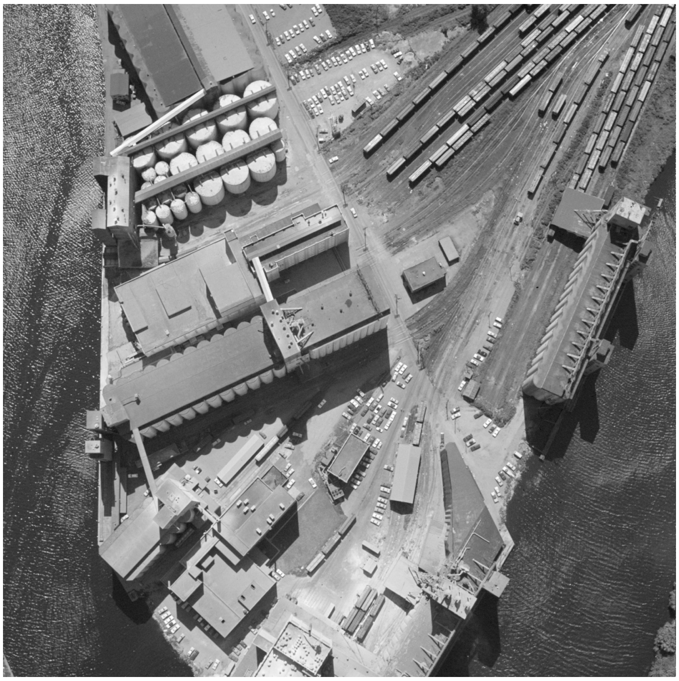


Fig. 8. Manipulated image. Vehicles around the building at the center have been removed.

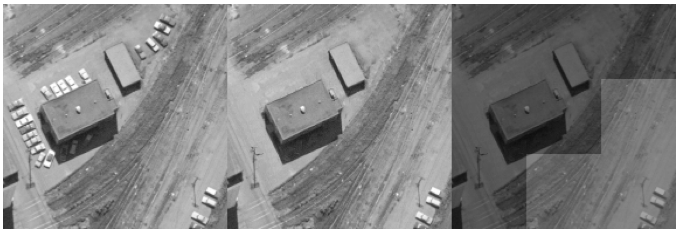


Fig. 10. Area of interest. Watermarked image, manipulated image, watermark detection result (left to right).

TABLE I

EFFECT OF *L-LAW* ON IMAGE QUALITY AND SUBSEQUENT LOSSLESS COMPRESSION. $\Delta_{\rm size}$ IS THE INCREASE IN THE COMPRESSED FILE SIZE

Image	PSNR (dB)	Δ_{size}(bytes)	$\frac{\Delta_{size}}{Payload}$	Δ_{size}(%)
F-16	56.54	2876	4.9	2.4
Mandrill	46.51	1440	2.5	0.8
Boat	52.91	2658	4.5	1.9
Barbara	52.91	2019	3.5	1.3
GoldHill	50.83	1819	3.1	1.2
Lena	52.83	1510	2.6	1.1
Average	52.09	2054	3.5	1.5

have been digitally removed. The altered image is shown in Fig. 8 (see Fig. 10 for an enlarged view of the area of interest). When that image is passed through the watermark detector, the image alteration has been successfully detected. Furthermore, the altered region has been located, as indicated by the darkest blocks in Fig. 9. In this figure, the shading reflects the level of confidence in the integrity of a particular block, light shading corresponding to high confidence values indicated by the hierarchical image authentication scheme [18].

A set of standard images (grayscale, 512 × 512 pixels) has been used to further evaluate the impact of the proposed algorithm on image quality and subsequent lossless compression. For each image, the PSNR value after embedding the 584 byte (sixty-four 64 × 64 and four 256 × 256 blocks with 64-bit MACs per block and a 320-bit DSA) payload required by our *L-LAW* implementation is shown in Table I. In addition to introducing a temporary embedding distortion, the lossless authentication watermarks often decrease the effectiveness of a subsequent lossless image compression step. As the watermarked image embodies both the image and the payload data, we expect an increase in the compressed file size equivalent to the payload size. While this observation should be true for a perfect coder, the corresponding increase in a typical coder is much larger than the payload size. In general, the watermark embedding step disturbs the image statistics in a manner that is not in agreement with the assumptions of the coder. As a result of the model mismatch, the coder encodes the watermarked image less efficiently. We quantify the effect of our algorithm on compression efficiency by reporting the change in the compressed (JPEG-LS [22]) file size, and the ratio of this increase to the payload size in Table I. Despite the three fold increase with respect to the payload size, the net increase with respect to the total (compressed) file size is around 1.5%. The additional functionality of the authentication watermarks often justifies this rather small increase.

V. Conclusion

We present a new lossless image authentication framework which offers computational efficiency, public/private key support and improved tamper-localization accuracy. The proposed framework is flexible and compatible with the existing lossless (reversible) data embedding and fragile image authentication algorithms. We have demonstrated a specific implementation of the framework using hierarchical image authentication and lossless G-LSB data embedding method. The framework can also be easily implemented using other fragile authentication and lossless data embedding methods, such as [13] and [23], respectively.

References

[1] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless authentication watermark LAW," *Proc. SPIE*, vol. 5020, pp. 689–698, Jan. 2003.

[2] A. Menezes, P. van Oorchot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1997.

[3] D. Stinson, *Cryptography: Theory and Practice*, 2nd ed. Boca Raton, FL: CRC, 2002.

[4] Information Technology-JPEG 2000 Image Coding System-Part 8: JPSEC, 2004.

[5] C. Podilchuk and E. Delp, "Digital watermarking: algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.

[6] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.

[7] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, no. 6, pp. 1064–1087, Jun. 1998.

[8] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data," *IEEE Signal Process. Mag.*, vol. 17, no. 5, Sep. 2000.

[9] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," *Proc. SPIE*, vol. 4314, pp. 197–208, Jan. 2001.

[10] C. Honsinger, P. Jones, M. Rabbani, and J. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," U.S. patent 6278791, Aug. 2001.

[11] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits, Syst., Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[12] J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5646997, 1997.

[13] J. Fridrich, M. Goljan, and A. Baldoza, "New fragile authentication watermark for images," presented at the *Proc. IEEE Int. Conf. Image Processing*, Sep. 2000.

[14] C. D. Vleeschouwer, J. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," in *Proc. IEEE 4th Workshop on Multimedia Signal Processing*, Oct. 2001, pp. 345–350.

[15] A. van Leest, M. van der Veen, and A. Bruekers, "Reversible watermarking for images," *Proc. SPIE*, vol. 5306, Jan. 2004.

[16] J. Dittmann, M. Steinebach, and L. Ferri, "Watermarking protocols for authentication and ownership protection based on timestamps and holograms," *Proc. SPIE*, vol. 4675, pp. 240–251, Jan. 2002.

[17] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[18] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.*, vol. 11, no. 6, pp. 585–595, Jun. 2002.

[19] J. Fridrich, "Security of fragile authentication watermarks with localization," *Proc. SPIE*, vol. 4675, no. 75, pp. 691–700, Jan. 2002.

[20] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[21] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. Image Process.*, vol. 9, no. 3, pp. 432–441, Mar. 2000.

[22] ISO/IEC 14495-1, Lossless and Near-Lossless Compression of Continuous-Tone Still Images-Baseline (JPEG-LS), 2000.

[23] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding- new paradigm in digital watermarking," *EURASIP J. Appl. Signal Processing*, vol. 2002, no. 2, pp. 185–196, Feb. 2002.

Mehmet Utku Celik (S'98–M'06) received the B.Sc. degree in electrical and electronic engineering in 1999 from Bilkent University, Ankara, Turkey, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Rochester, Rochester, NY, in 2001 and 2004, respectively.

Currently, he is with the Information and Systems Security Department, Philips Research, Eindhoven, The Netherlands. His research interests include digital watermarking and data hiding—with emphasis on multimedia authentication—image and video processing, and cryptography.

Dr. Celik is a member of the ACM and the IEEE Signal Processing Society.

Gaurav Sharma (S'88–M'96–SM'00) received the B.E. degree in electronics and communication engineering from Indian Institute of Technology Roorkee (formerly the University of Roorkee), India, in 1990, the M.E. degree in electrical communication engineering from the Indian Institute of Science, Bangalore, in 1992, and the M.S. degree in applied mathematics and the Ph.D. degree in electrical and computer engineering from North Carolina State University (NCSU), Raleigh, in 1995 and 1996, respectively.

From August 1992 to August 1996, he was a Research Assistant at the Center for Advanced Computing and Communications, Electrical and Computer Engineering Department, NCSU. From August 1996 to August 2003, he was with Xerox Research and Technology, Webster, NY, initially as a Member of Research Staff and subsequently in the position of Principal Scientist. Since Fall 2003, he has been an Associate Professor with the University of Rochester, Rochester, NY. His research interests include multimedia security and watermarking, color science and imaging, signal restoration, and halftoning.

Dr. Sharma is a member of Sigma Xi, Phi Kappa Phi, Pi Mu Epsilon, IS&T, and the IEEE Signal Processing Society. He was the 2003 Chair for the Rochester Chapter of the IEEE Signal Processing Society and is the Treasurer for the Rochester Section. He currently serves as an Associate Editor for the IEEE Transactions on Image Processing, IEEE Transactions on Information Forensics and Security, and the *Journal of Electronic Imaging*.

A. Murat Tekalp (S'80–M'84-SM'91–F'03) received the M.S. and Ph.D. degrees in electrical, computer, and systems engineering from Rensselaer Polytechnic Institute (RPI), Troy, NY, in 1982 and 1984, respectively.

From December 1984 to August 1987, he was with Eastman Kodak Company, Rochester, NY. He joined the Electrical and Computer Engineering Department at the University of Rochester in September 1987, where he is currently a Distinguished Professor. Since June 2001, he also has been with Koc University, Istanbul, Turkey. His research interests are in the areas of digital image and video processing, including video compression and streaming, video filtering for high-resolution, video segmentation, object tracking, content-based video analysis and summarization, multicamera surveillance video processing, and protection of digital content. He authored the book *Digital Video Processing* (Prentice-Hall, 1995). He holds five U.S. patents. His group contributed technology to the ISO/IEC MPEG-4 and MPEG-7 standards.

Dr. Tekalp was named a Distinguished Lecturer by the IEEE Signal Processing Society in 1998. He has chaired the IEEE Signal Processing Society Technical Committee on Image and Multidimensional Signal Processing (January 1996 to December 1997). He has served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING (1990 to 1992), IEEE TRANSACTIONS ON IMAGE PROCESSING (1994 to 1996), and the *Journal Multidimensional Systems and Signal Processing* (1994 to 2002). He was an area editor for the *Journal of Graphical Models and Image Processing* (1995 to 1998). He was also on the editorial board of the *Journal of Visual Communication and Image Representation* (1995 to 2002). He was appointed as the Technical Program Chair for the 1991 IEEE Signal Processing Society Workshop on Image and Multidimensional Signal Processing, the Special Sessions Chair for the 1995 IEEE International Conference on Image Processing, the Technical Program Co-Chair for IEEE ICASSP 2000, Istanbul, Turkey, and the General Chair of IEEE International Conference on Image Processing (ICIP), Rochester, in 2002. He is the Founder and first Chairman of the Rochester Chapter of the IEEE Signal Processing Society. He was elected as the Chair of the Rochester Section of IEEE from 1994 to 1995. At present, he is the Editor-in-Chief of the *EURASIP Journal on Image Communication*.