Secure Block-Based Video Authentication with Localization and Self-Recovery

Ammar M. Hassan, Ayoub Al-Hamadi, Yassin M. Y. Hasan,
Mohamed A. A. Wahab, and Bernd Michaelis

***Abstract*—**Because of the great advance in multimedia technology, digital multimedia is vulnerable to malicious manipulations. In this paper, a public key self-recovery block-based video authentication technique is proposed which can not only precisely localize the alteration detection but also recover the missing data with high reliability. In the proposed block-based technique, multiple description coding MDC is used to generate two codes (two descriptions) for each block. Although one block code (one description) is enough to rebuild the altered block, the altered block is rebuilt with better quality by the two block descriptions. So using MDC increases the ratability of recovering data. A block signature is computed using a cryptographic hash function and a doubly linked chain is utilized to embed the block signature copies and the block descriptions into the LSBs of distant blocks and the block itself. The doubly linked chain scheme gives the proposed technique the capability to thwart vector quantization attacks. In our proposed technique , anyone can check the authenticity of a given video using the public key. The experimental results show that the proposed technique is reliable for detecting, localizing and recovering the alterations.

***Keywords*—**Authentication, hash function, multiple description coding, public key encryption, watermarking.

I. Introduction

MANY recently developed tools and efficient software products offer clients worldwide capabilities of flexibly creating, manipulating, and exchanging multimedia data. So, effective methods are required for guaranteeing privacy, security, protection and integrity of the various multimedia data categories. Considerable efforts are introduced on digital watermarking for many purposes such as multimedia authentication and copyright protection [1]-[5]. Watermarking techniques, that insert a piece of information (the watermark) into multimedia (host/cover) data, may be classified based on their tradeoffs of the following central differing properties: robustness, blindness, transparency, security, capacity and complexity.

Multimedia authentication involves confirmation of the detection of multimedia content modifications, with precisely localized alteration detection, independent of the multimedia format [5]-[6]. Various fragile, semi-fragile and robust methods have been introduced for multimedia authentication. The high sensitivity of fragile marks make them attractive for authentication. Hence, fragile authentication is applicable and of interest in case of lossless environment, i.e., coding, storage, transmission (of the authenticated multimedia).

Different fragile image authentication methods have been introduced [3]-[8]. A simple fragile method only replaces the least significant bits (LSBs) of the image of interest with the checksum (i.e., modulo-2 addition) bits of a long word of some most significant bits (MSBs) [7]. Wong algorithm [4] is the cornerstone of blockwise image authentication algorithms. It divides the image into nonoverlapping blocks. Then, for each block, the block signature is computed using a public key hash function and inserted into the LSBs of the block itself. On the other hand, semifragile watermarking techniques [9]-[11] embed watermarks so robustly to survive (to some, application dependent, extend) various kinds of typical image processing manipulations such as lossy compression, histogram equalization, filtering, scaling, rotation, and mild cropping operations as long as the image content are preserved. Self-embedding authentication techniques, that embed an image approximation/visual hash [12]-[16] into the image itself, have been introduced to not only localize altered regions but also reconstruct the alteration detection.

video authentication can be considered similar to image authentication where a video is a sequence of images (frames). In particular, image authentication is applied on each frame individually [17]. In [18], an object-based video authentication technique has been introduced. Error correction coding and cryptographic hashing are applied to selected angular radial transformation coefficients to produce the watermark. Then, this watermark is embedded into the objects frame by frame using randomly selected discrete Fourier transformation coefficients. For H.264/AVC compressed video, video authentication techniques have been proposed in [19]-[20].

The fundamental objective of the attacker facing such fragile watermark is to keep a watermark that makes his

A. M. Hassan, A. Al-Hamadi, and B. Michaelis are with Institute for Electronics, Signal Processing and Communications (IESK), Otto-von-Guericke-University, Magdeburg, Germany (e.mail: {Ayoub.Al-Hamadi, Ammar-Mostafa.Ammar}@ovgu.de).

Y. M. Y. Hasan is with the Computer Science and Information Dept., Taibah University, Madina, Saudi Arabia.

M. A. A. Wahab is with the Electrical Engineering Department, Minia University, Minia, Egypt.

altered or completely forged image, “pass” the verification test as authentic. This type of attack principally differs from the attacks against copyright protection and information hiding where the attacker may mainly want to significantly distort or remove the watermark with imperceptible alterations in the image [21]-[23].

In [21], An attack on block-based independent authentication techniques has been proposed, referred to as vector quantization (VQ) or collage attack. In this attack technique, the attacker can fabricate a counterfeiting image (perceptually indistinguishable) or deliberately introduce imperceptible changes only to some local original information in a authenticated image. The VQ attack constructs a VQ codebook using original authenticated images which have the same size and authenticated with the same key. The attacker can search and find the best match for a given unauthenticated block.

In this paper, a public key self-recovery video authentication technique, thwarting vector quantization attacks, is proposed. The technique is capable of localizing the alteration detection and restoring the missing data.

II. Existing Self-Recovery Schemes

An original self-recovery/embedding image authentication technique based on JPEG compression has been introduced in [15]. JPEG compressed version of each block B is inserted into the LSBs of the block $B+\vec{P}$, where $\vec{P}$ is a vector of length approximately 1/3 of the image size, with a randomly chosen direction. The algorithm limitations and possible attacks are addressed in [16]-[24]. The serious problem is that the attacker can replace the block B by another authenticated block say D and also replace the LSBs of block $B+\vec{P}$ by the LSBs of the block $D+\vec{P}$. Thus, the algorithm has a shortcoming in the alteration detection.

Another algorithm has been proposed using quantized coefficients of the DCT of the image blocks as a watermark and modifying the coefficients differences to match the quantized coefficients (watermark) [25]. The attacker can easy defeat the verification process applying the same algorithm into a fake image.

In [24], an algorithm uses a halftone version of the host image instead of using the JPEG compression version. The halftone image is pixel-wise permuted using a random generator and embedded into the LSBs of the original image. The security of this algorithm lies in the key of the random generator which may be detected using the cryptographic analysis when the attacker has many authenticated images [26]-[27].

Fractal codes of the ROI (region of interest) ,which is chosen as the important object in the image, are used as an approximated version of the ROI [28]. The codes and a watermark are inserted into the LSBs of the host image. In this algorithm, the ROI should be exactly known in the verification process. Furthermore, the fractal codes are not protected where the attacker can easily counterfeit an image without triggering the verification process.

In [3], a hybrid image authentication technique has been proposed which includes a fragile scheme for sensitive authentication and a robust self-embedding scheme for self-correction. The problem of this algorithm is the low quality of the authenticated image. A block-based video authentication scheme with self-recovery has been introduced in [17]. The watermark payload of a block has two parts: authentication and recovery packets. The block watermarks are embedded into arbitrary distant blocks. The technique uses a private key for both embedding and verification process.

III. Proposed technique

We produce a novel solution for video authentication using multi linked chain approach, multiple description coding and public key cryptography. To thwart the vector quantization attack, multi linked chain technique is used where the signature of a block is embedded into multiple distant blocks and the block itself. Multiple description block coding is utilized for increasing the reliability of altered block recovery. Public key encryption is a tool for the security of the proposed algorithm where the video owner uses a privet key in the embedding process and the video authenticity is checked using the public key. The proposed technique is fragile blockwise video authentication which is so sensitive to tiny changes in pixel values and it is capable of localizing the alterations. The self recovery capability is useful when some blocks or regions are altered. In this case, the technique can approximately restore the original blocks or regions. The proposed authentication technique has two major processes, the embedding process and the verification process which will be explained in the next subsections.

A. Embedding Process

The goal of the embedding process is to insert a block signature copy into the block itself and insert two block signature copies and two block codes (two descriptions) into distant blocks. Fig. 1(a) illustrates the main operations for the embedding process. The first stage, we divide all farms into equal blocks. For each block, we generate two indices for two distant blocks. Then, the block signature and block descriptions are computed. For security reason, the blocks signatures and the blocks codes which will embedded in the LSBs of a block are encrypted using a public key encryption algorithm. The authenticated video is obtained after embedding the encrypted signatures copies/blocks codes into the LSBs of the distant blocks and the block itself. We can note that the block signature is embedded into two distant blocks and the signature of those distant blocks are embedded into other distant blocks and so on, making a doubly linked chain for all blocks.

Frame dividing and indices generation

Consider the video *V* which contains F_n $M \times N$ frames. Each frame is dividing into $n\times n$ blocks to constructed the vector V_b such that

$$V_b = \left\{ B_{I^3_1}, B_{I^3_2}, ..., B_{I^3_i}, ..., B_{I^3_{Fn\times N_b\times M_b}} \right\} I^3_i = \left(I_f, I_r, I_c \right) \qquad (1)$$

where :

B is a n×n block,
I_f is the frame index,
I_r is the row index of the frame I_f,
I_c is the column index of the frame I_f,
M_b is the number of blocks per column in each frame,
N_b is the number of blocks per row in each frame.

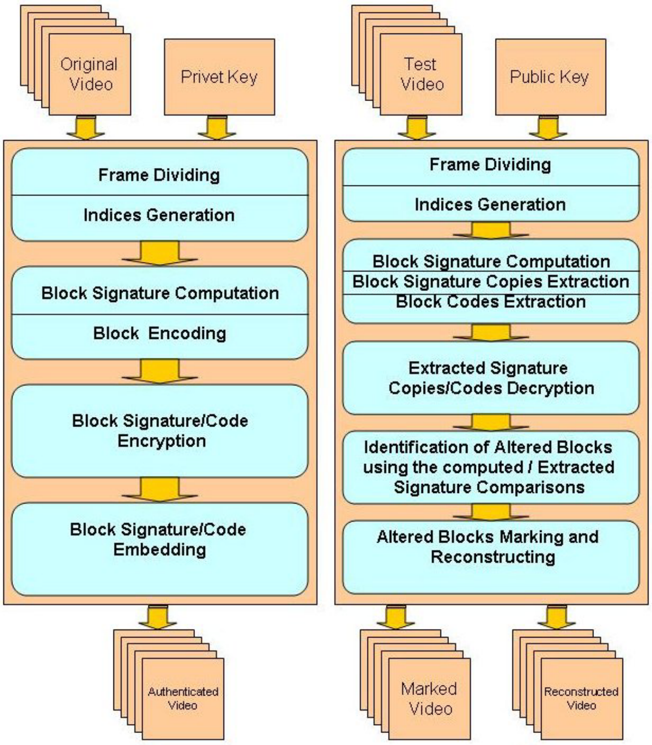
Original Video
Privet Key
Frame Dividing
Indices Generation
Block Signature Computation
Block Encoding
Block Signature/Code Encryption
Block Signature/Code Embedding
Authenticated Video
Test Video
Public Key
Frame Dividing
Indices Generation
Block Signature Computation
Block Signature Copies Extraction
Block Codes Extraction
Extracted Signature Copies/Codes Decryption
Identification of Altered Blocks using the computed / Extracted Signature Comparisons
Altered Blocks Marking and Reconstructing
Marked Video
Reconstructed Video
(a)
(b)

Fig.1. Proposed video authentication. (a) Embedding process. (b) Verification process.

For each block $I^3_i=(I_f, I_r,I_c)$, two indices for two distant blocks I^3_j, I^3_k are computed as follows:

$$\begin{aligned} I_{jf} &= VI_1(I_f) \\ I_{kf} &= VI_2(I_f) \\ I_{jr} &= \left(I_r + G_1(I_c)\right) \bmod M_b \\ I_{jc} &= \left(I_c + G_1(I_r)\right) \bmod N_b \\ I_{kr} &= \left(I_r + G_2(I_c)\right) \bmod M_b \\ I_{kc} &= \left(I_c + G_2(I_r)\right) \bmod N_b \end{aligned} \qquad (2)$$

where:

Vl_1, Vl_2 are two interleaves of the vector $\{0,1,2,...,F_n-1\}$,
G_1 and G_2 are seed random generators.

If we use keyed random generators, the used keys are public keys (known for all).

Block descriptions

For each block of a frame, DCT is computed. Then, chosen low frequency DCT coefficients and the DC are quantized and encoded using a JPEG quantization table and a fixed bit allocation table, respectively. Then, from encoding data, we construct two groups $E1$ and $E2$ where $E1 \cup E2$ cantinas all encoding data and $E1 \cap E2$ contains at least the DC code. $E1$ and $E2$ are multiple description coding (MDC) of the block (two descriptions). In MCD approach, the reconstruction block can be rebuilt with one block code (description). If both block codes (two descriptions) exist, the block is rebuilt with low distortion.

Block signature

The block signature is computed as a hashing of the MSBs of block pixels and the block index using a hash function such as N-Hash, MD4, MD5, SHA, etc. The output of a hash function D (digest) may have a long fixed length dependent on the specific hash function used. To reduce the digest length, we can choose specific bits as a signature or divide the digest into many equal parts and xoring them. So, the block signature vector V_s is computed as follows:

$$D_{I^3_i} = H(MSBs, I^3_i) \qquad (3)$$

$$S_{I^3_i} = f(D_{I^3_i}) \qquad (4)$$

$$V_s = \{S_{I^3_1}, S_{I^3_2}, ...; S_{I^3_{F_n\times M_b\times N_b}}\} \qquad (5)$$

Then, we build a vector V_{LSB} containing the blocks signatures and the blocks descriptions that will be inserted into the LSBs of the blocks. The vector element $V_{LSB}(I^3_i)$ is divided into five fields, one for the signature copy of the block itself, two fields for the signature copies of the distant blocks, and the last two fields for the two blocks descriptions. So, V_{LSB} is computed such that

$$\begin{aligned} V_{LSB}(I^3_i)\big|field1 &= S_{I^3_i} \\ V_{LSB}(I^3_j)\big|field2 &= S_{I^3_i} \\ V_{LSB}(I^3_k)\big|field3 &= S_{I^3_i} \\ V_{LSB}(I^3_j)\big|field4 &= E1_{I^3_i} \\ V_{LSB}(I^3_k)\big|field5 &= E2_{I^3_i} \end{aligned} \qquad (6)$$

After the V_{LSB} is completely constructed, each vector element $V_{LSB}(I^3_i)$ is encrypted using a public key encryption algorithm and inserted into the LSBs of the bock I^3_i as follows:

$$LSBs(B_{I^3_i}) = Encrypt_{Ke}(V_{LSB}(I^3_i)) \qquad (7)$$

where Ke is a private key.

B. Verification Process

Fig. 1(b) demonstrates the verification process steps. The test video V' is divided into blocks V'_b as in (1) and distant blocks indices are computed for each block using (2). For each block, the block signature is computed by (3) and (4) forming the computed signature vector $V's$. Then, we extract the signature copies and the block descriptions for each block to construct *Ve* such that:

$$V_e(I_i^3) = decrypt_{Kv}(LSBs(V_b'(B_{I_i^3}))) \qquad (8)$$

where *Kv* is the public key.

The block is an altered block if its computed signature is mismatch with the extracted signature from the block itself or mismatch with the both extracted signature copies from the distant blocks. So, a vector V_v containing the blocks authenticity is computed as follows:

$$V_v(I_i^3) = \begin{cases} 1, \; V_s(I_i^3) = V_e(I_i^3) \mid field1 = V_e(I_j^3) \mid field2 \\ \quad or\; V_s(I_i^3) = V_e(I_i^3) \mid field1 = V_e(I_k^3) \mid field3 \\ 0, \; otherwise \end{cases} \qquad (9)$$

where I^3_j and I^3_k are computed using (2).

Block reconstruction

For each altered block , we check the status of the distant blocks if at least one of them is not altered, the block code (description) embedded in it is extracted and used for rebuilding the block. Sure, if both distant blocks are not altered, we can extract the two block codes (two descriptions) and can rebuild the block with better quality. There is a possibility of lost the block forever if both distant blocks are altered. In this case , the reconstructed block is remarked as a lost bock. The vector *Vr* containing the reconstructed blocks which is used for reconstructing the video, is computed such that

$$Vr(I_i^3) = \begin{cases} dec1(V_e(I_j^3 \mid field4), \; V_v(I_i^3) = 0 \\ \qquad and\; V_v(I_j^3) = 1 \;and\; V_v(I_k^3) = 0 \\ dec2(V_e(I_k^3 \mid field5), \; V_v(I_i^3) = 0 \\ \qquad and\; V_v(I_j^3) = 0 \;and\; V_v(I_k^3) = 1 \\ dec3(V_e(I_i^3 \mid field4, I_k^3 \mid field5), \; V_v(I_i^3) = 0 \\ \qquad and\; V_v(I_j^3) = 1 \;and\; V_v(I_k^3) = 1 \\ B_{lost}, V_v(I_i^3) = 0 \;and\; V_v(I_j^3) = 0 \;and\; V_v(I_k^3) = 0 \\ V_b'(I_i^3), \; V_v(I_i^3) = 1 \end{cases} \qquad (10)$$

where:

B_{lost} is a $n \times n$ block marked as a lost block,
dec1, dec2 and *dec3* are three block decoding methods.

IV. Experimental Results

In order to validate the proposed authentication system, we tested it using several test videos. The proposed technique is apparently capable of detecting local alterations attacks and VQ attacks which replace contiguous blocks by blocks coming from different frames regions. Thus, we will consider an example to demonstrate the performance in case of a large region in a frame coming from another authenticated frame (we can repeat this case for many frames). We use RSA as a public key algorithm and SHA (Secure Hash Algorithm) as a hash function. The used block size is 8×8 and two LSB plans are exploited for embedding blocks descriptions and signatures copies. We applied the proposed algorithm on the three channels of the test video which has 480×640 frames.

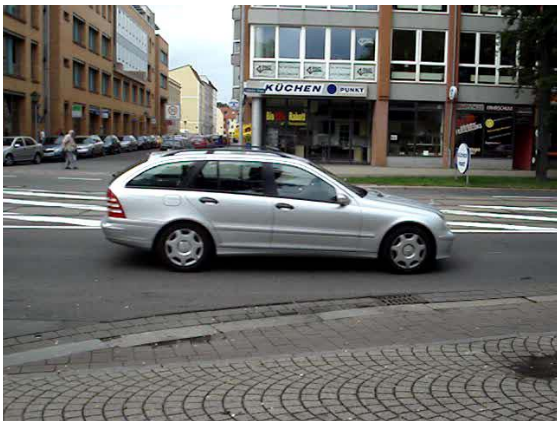

Fig.2 Original frame.

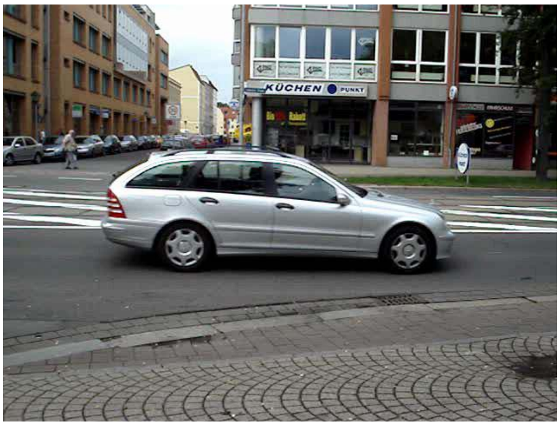

Fig.3 Authenticated frame using the proposed technique. Correlation coefficient=0.9998, PSNR=46.64 dB.

Assume that an attacker removes an object from the authenticated video and places, instead of the removed object, adjacent blocks coming from another authenticated area. Fig. 2 is the original frame and Fig. 3 is the authenticated version. The computed peak signal to noise ratio PSNR and correlation coefficient between the original and authenticated frames are 46.64dB and 0.9998, respectively. In Fig. 4, the car object is removed and precisely replaced by a background coming from another authenticated frame without introducing perceptually noticeable difference. Fig. 5 shows that the proposed technique succeeded in effectively detecting and localizing the alterations. The reconstructed frame is shown in Fig. 6. The proposed method efficiently recovered the missed car object where PSNR and correlation coefficient between the reconstructed and the original fames are 33.15dB and 0.9939, respectively.

V. Conclusion

A novel public key self-recovery video authentication technique is proposed. The proposed method is not only capable of localizing the alteration detection but also capable of recovering the missing contents with high reliability using multiple description coding. Furthermore, the proposed technique thwarts VQ attacks using a multiple links chain to securely embed the block signature copies into several arbitrary-distant blocks. Public key algorithms are utilized for guaranteeing the security and permitting anyone to test the authenticity of a given video.

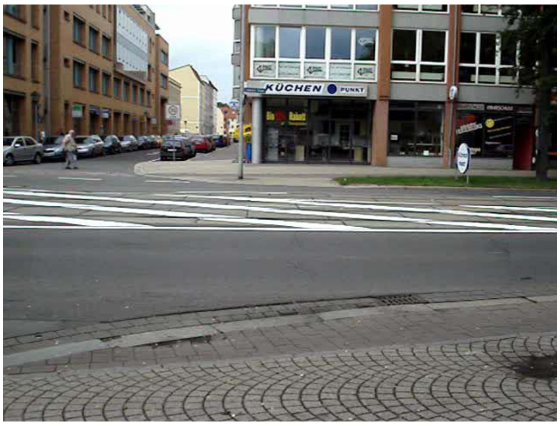

Fig. 4 Altered version of the authenticated frame.

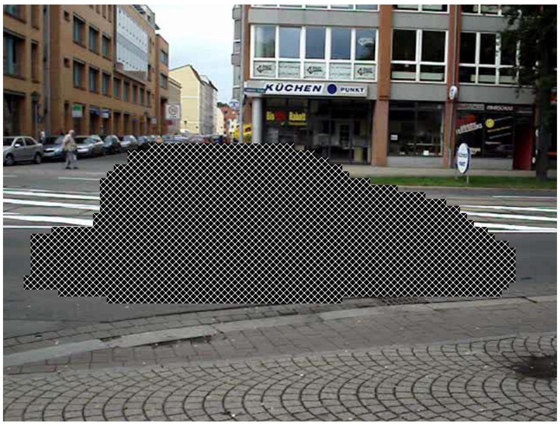

Fig. 5 Verification result marking the altered blocks.

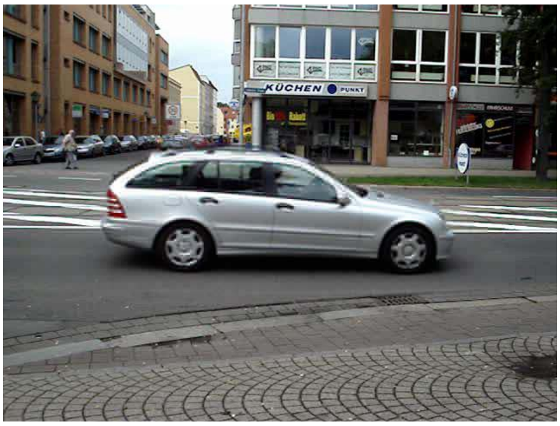

Fig. 6 Verification result reconstructing the altered blocks. Correlation coefficient=0.9939, PSNR=33.15 dB.

Acknowledgment

This work is supported by Forschungspraemie (BMBF-Förderung, FKZ: 03FPB00213) and Transregional Collaborative Research Centre SFB/TRR 62 ”Companion-Technologyfor Cognitive Technical Systems” funded by the German Research Foundation (DFG).

References

[1] C. Fei, D. Kundur and R. H. Kwong, "Analysis and design of secure watermark-based authentication system," *IEEE Trans. on Information Forensics and Security*, vol.1, no.1, pp.43-55, March 2006.

[2] Y. M. Y. Hasan and A. M. Hassan, “Dual domain localized autorecovery image authentication," *in Proc. Information Security Symposium (ISS'06)*, Al-Madina, KSA, May 2-4, 2006, pp.138-148.

[3] P. W. Wong, “A public key watermark for image verification and authentication,” *in Proc. ICIP*, NY, USA, Oct.4-7, 1998, pp.425–429.

[4] P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” *IEEE Trans. on Image Proc.*, vol.10, no.10, Oct. 2001.

[5] Y. M. Hasan and A. M. Hassan, “Tamper detection with self-correction hybrid spatial-DCT domains image authentication technique,” *in Proc. IEEE ISSPIT'07*,Cairo, Egypt, 2007.

[6] Y. M. Y. Hasan and A. M. Hassan, “Fragile blockwise image authentication thwarting vector quantization attack,” *in Proc. IEEE ISSPIT'04*, Rome, Italy, Dec. 18-21, 2004, pp.530-533.

[7] E. Lin and E. Delp, “A review of fragile image watermarks,” *in Proc. of the ACM Multimedia and Security Workshop*, 1999, pp. 25-29.

[8] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "A hierarchical image authentication watermark with improved localization and security," *in Proc. ICIP'01*, Greece, Oct. 2001, pp.502-505.

[9] E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of image alterations using semi-fragile watermarks," *in Proc. of the SPIE Int. Conf. on Security and Watermarking of Multimedia Contents II*, vol. 3971, San Jose, CA, USA, Jan. 23 - 28, 2000.

[10] O. Ekici, B. Sankur, B. Coskun, U. Naci and M. Akcay, “Comparative evaluation of semi-fragile watermarking algorithms,” *Journal of Electronic Imaging*, vol.13, no.1, pp.209-216, Jan. 2004.

[11] K. Al-sultan, M. Saeb and U. Badawi, “A proposed semi-fragile watermarking scheme for image authentication," *in Proc. ICCTA'04,* Alexandria, Egypt, Sep.6-9, 2004.

[12] J. Fridrich, "Robust bit extraction from images," *in Proc. IEEE ICMCS'99,* Florence, Italy, vol. 2, June 7-11, 1999, pp.536-540.

[13] J. Fridrich, "Visual hash for oblivious watermarking," *in Proc. SPIE Photonic West Electronic Imaging: Security and Watermarking of Multimedia Contents*, San Jose, U.S.A., Jan. 24-26, 2000, pp.286–294.

[14] J. Fridrich, M. Goljan, "Robust hash functions for digital watermarking," *in Proc. ITCC*, CA, USA, March 2000, pp.173–178.

[15] J. Fridrich and M. Goljan, “Images with self-correction capabilities,” *in Proc. ICIP'99*, Kobe, Japan, 1999.

[16] J. Fridrich and M. Goljan, “Protection of digital images using self embedding,” *Symp. Content Security and Data Hiding in Digital Media*, New Jersey Institute of Technology, May 14, 1999.

[17] M. Celik, Gaurav , G. Sharma, A. M. Tekalp , E. Saber, " Video authentication with self recovery," *Proceedings of SPIE, Security and atermarking of Multimedia Content IV*, vol 4675. San Jose, CA, USA , pp 531-541, 2003.

[18] D. He, Q. Sun, and Q. Tian, "A secure and robust object-based video authentication system," *EURASIP Journal on Applied Signal Processing,* vol. 2004, Issue 14, PP 2185-2200, Jan. 2004.

[19] D. Pröfrock, H. Richter, M. Schlauweg, E. Müller, "H.264/AVC video authentication using skipped macroblocks for an erasable watermark, " *Proc. of the VCIP*, Beijing, China, July 2005.

[20] N. Ramaswamy, K. R. Rao, "Video authentication for H.264/AVC using digital signature standard and secure hash algorithm, " *Proceedings of the 2006 international workshop on Network and Operating Systems Support for Digital Audio and Video 2006*, Newport, Rhode Island November 22 - 23, 2006.

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

[22] M. Kutter, S. Voloshynovskiy znd A. Herrigl, “The watermark copy attack,” *in Proc. SPIE Elect. Imaging*, San Jose, USA, Jan. 23-28, 2000.

[23] D. Kirovski and F. A. P. Petitcolas, “Blind pattern matching attack on watermarking systems,” *IEEE Trans. on Signal Processing*, pp.1-9, 2002.

[24] H. Lue, Z. Lu, S. Chu, and J. Pan, “Self embedding watermarking scheme using halftone image,” IIEICE Transactions on Information and Systems, 2008.

[25] C. Lin and S. F. Chang, “SARI: self-authentication-and-recovery image watermarking system,” *Proceedings of the ninth ACM Conference on Multimedia*, Ottawa, Canada ,2001.

[26] A. J. Menezes, P. C. Orschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.

[27] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, USA, 1996.

[28] S. Wang and S. Tsai, “Automatic image authentication and recovery using fractal code embedding and image inpainting,” *Journal of the Pattern Recognition Society*, vol. 41, pp. 701 – 712, 2008.