International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:7, 2008

Embedded Semi-Fragile Signature Based Scheme for Ownership Identification & Color Image Authentication with Recovery

M. Hamad Hassan, and S.A.M. Gilani

Abstract**—**In this paper, a novel scheme is proposed for *Ownership Identification* and *Color Image Authentication* by deploying *Cryptography & Digital Watermarking.* The color image is first transformed from *RGB* to *YST* color space exclusively designed for watermarking. Followed by color space transformation, each channel is divided into 4×4 non-overlapping blocks with selection of central 2×2 sub-blocks. Depending upon the channel selected two to three *LSBs* of each central 2×2 sub-block are set to zero to hold the ownership, authentication and recovery information. The size & position of sub-block is important for correct localization, enhanced security & fast computation. As $YS \perp T$ so it is suitable to embed the recovery information apart from the ownership and authentication information, therefore 4×4 block of *T* channel along with ownership information is then deployed by *SHA160* to compute the content based hash that is unique and invulnerable to birthday attack or hash collision instead of using *MD5* that may raise the condition i.e. $H(m) = H(m')$. For recovery, intensity mean of 4x4 block of each channel is computed and encoded upto eight bits. For watermark embedding, key based mapping of blocks is performed using *2D-Torus Automorphism.* Our scheme is oblivious, generates highly imperceptible images with correct localization of tampering within reasonable time and has the ability to recover the original work with probability of near one.

Keywords**—**Hash Collision, LSB, MD5, PSNR, SHA160

I. Introduction

IN past few years, there has been exponential growth in the use of digital multimedia contents. The internet made it easy & fast to exchange the multimedia contents. But, the availability of modern image processing tools threatened the image authenticity, by letting the user to do even imperceptible changes in the original work.

Manuscript received on April 30, 2006. This work was supported in part by the HEC, Pakistan under faculty development program.

M. Hamad Hassan is graduate student of Faculty of Computer Science & Engineering at GIK Institute, Pakistan (email: hamad_gikian@yahoo.com).

Dr. Asif Gilani is the Dean of Faculty of Computer Science & Engineering at GIK Institute, Pakistan (email: asif@ giki.edu.pk).

Hash Collision: when two messages have same hash
LSB: Least Significant Bits, PSNR: Peak Signal to Noise Ratio,
MD5: Message Digest, SHA: Secure Hash Algorithm

Authentication verifies the integrity of an original work. In this regard, digital watermarking gave promising solution for ownership identification and authentication of work using digital images, audio, video or text document. The principle authentication schemes are briefly discussed here: Manuscript received on April 30, 2006. This work was supported in part by the HEC, Pakistan under faculty development program.

Selective Authentication System (SAS): The system that verifies that work has not been modified by any of a predefined set of illegitimate distortions, while allowing modifications by legitimate distortions. To implement ***SAS*** three basic approaches are followed:

Semi Fragile Watermarks (SFW): These are designed to survive legitimate distortions but destroyed by the illegitimate distortions.

Semi Fragile Signatures (SFS): These are signatures computed from the properties of the work that are unchanged by legitimate distortions and secure than *SFW* because they are not vulnerable to copy attack.

Tell Tale Watermarks (TTW): Theses are designed to be examined in detail after the work is modified. By determining how the watermark has been changed, we can infer how the work has been destroyed and make a subsequent determination as to whether or not the distortion was legitimate.

Instead of separately storing the authentication data, the watermarking based schemes embed the data into the original work [7]-[10] which is twofold; firstly it becomes the integral part of original work, secondly it takes less memory for processing and storage, transmission is fast and security is relatively high. The watermarking based scheme is sensitive to any modification that tries to alter the contents of original image & can be authenticated by embedding a watermark in it. In past several researchers have presented content based signature schemes for content authentication and ownership identification.

In this paper, a novel scheme is proposed for *Ownership Identification* and *Color Image Authentication* with the ability to recover the original work. The proposed scheme deploys *Cryptography & Digital Watermarking* to have single solution for *Ownership Identification and Authentication.*

The given color image that will proof the ownership is first transformed from *RGB to YST* color space, exclusively designed & recommended for watermarking based applications by Francesco et al. [2]. Followed by color space transformation, each channel is divided into 4×4 non-overlapping blocks & its central 2×2 sub-block is selected. In case of *YS* channels only two *LSBs* of each central 2x2 sub-block, are set to zero, to hold the recovery information but in case of *T* channel three *LSBs* of each central 2×2 sub-block are set to zero, to hold the ownership information apart from the recovery information.

Geometrically $YS \perp T$ and therefore *T* channel gave us liberty to embed more bits. The size & position of sub-block is important for correct localization, enhanced security & fast computation.

The 4×4 non-overlapping block of *T* channel along with ownership information is then deployed by *SHA160* to compute, content based hash that is unique and invulnerable to birthday attack or hash collision, as recommended by *RSA Data Security Inc & B. Schneier* [4]-[5] rather than *MD5* that may raise the condition i.e. $H(m) = H(m')$ where two different messages can have the same hash.

For recovery, intensity mean of 4×4 block of each channel is computed and encoded upto 8 bits. The target block that will hold the source block information is determined by implementing *2D-Torus Automorphism* presented by G. Voyatzis et al. [6] using private key to have secure mapping of blocks. The quality of watermarked images is quite reasonable both subjectively and objectively. Our scheme is oblivious, correctly localizes the tampering in a work within reasonable time and with the ability to recover the original work of probability near one.

The rest of paper is organized as: Section II summarizes the related work. Section III explains the proposed scheme. Section IV demonstrates the simulation results and Section V presents the concluding remarks.

II. Related Work

Walton [11] uses a key dependent pseudo-random walk on the image. The check-sum is obtained by summing the numbers determined by the seven most significant bits (*MSB*) and taking a remainder with a large integer *N*. The check-sum is inserted in a binary form in the *LSBs* of selected pixels. The method is very fast and on average modifies only half of the pixels by one gray level. Check-sums provide a very high probability of tamper detection, but cannot distinguish between an innocent adjustment of brightness and replacing a person's face.

Van Schyndel et al. [12] modify the *LSBs* of pixels by adding extended m-sequences to the rows of pixels. The sequences are generated with a linear feedback shift register. For an *N*×*N* image, a sequence of length *N* is randomly shifted and added to the image rows. The phase of the sequence carries the watermark information. A simple cross-correlation is used to test for the presence of the watermark which is obviously not sufficient way, in case if someone desires to recover the original work from the tampered area of the image.

Wolfgang and Delp [13] extended van Schyndel's work and improved the localization properties and robustness. They mapped a binary sequence from {0,1} to {-1,1} and embed that sequence into the selected image blocks. They embedded the watermark into the *LSBs* of the pixels that can be easily removed.

Chang C.C, Hu Y.S. & Lu T.C. [1] extended Wolfgang and Delp work and presented the scheme for authentication of gray scale images by deploying *MD5* one way hash function. Their proposed scheme works fine for the authentication of gray scale images but as recommended by *RSA Data Security Inc and B. Schneier* [4]-[5] it may raise the condition i.e. $H(m) = H(m')$. Also the block size is adequate for localization of tamper detection but computationally inadequate in terms of hash computation. In addition there was need to recover the original work. Therefore a scheme is proposed to have a single solution for issues discussed earlier with the following distinct features.

i) Color space suitable for watermark embedding, for that *YST* color space is deployed.

ii) To have an authentication system that is computationally fast but with better localization of tampered region, for that non-overlapping block of size 4×4 is chosen.

iii) Geometrically $YS \perp T$ and therefore gives degree of freedom to embed more bits, that's why *T* channel is selected to hold ownership information apart from recovery information while the *YS* channels only holds the recovery information.

iv) For watermark embedding each channel's 4×4 block central 2×2 sub-block is selected and in case of *YS* channels two *LSBs* are set to zero but in case of *T* channel three *LSBs* are set to zero.

v) For ownership identification, *SHA160* is deployed that computes the unique hash by deploying all the twelve neighboring pixels of each 4×4 block of *T* channel along with ownership information like owner id, time stamp, private key etc. To control the length of hash bits, bit level *XOR* operator is applied to have unique bits upto desired length.

vi) For recovery of work, intensity mean of each 4×4 block is computed.

vii) The hash bits and the intensity mean bits are then concatenated to have the watermark bits.

viii) To have secure mapping of blocks, to hold watermark information, *2D Torus Authomorphism* is implemented with a private key.

III. Proposed Shceme

Pre-Processing of Image:

Let *C* be the color image in *RGB* color space with size *M*×*N*. This color image is first transformed from *RGB* to *YST* color space using the set of linear transformation matrix given by equation (1).

$$\begin{vmatrix} Y \\ S \\ T \end{vmatrix} = \begin{vmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{vmatrix} . \begin{vmatrix} R \\ G \\ B \end{vmatrix} \quad (1)$$

Watermark Generation & Embedding

1. Select each channel and divide it into 4×4 non-overlapping blocks.

2. Select the central 2×2 sub-block of each 4×4 block of each channel and in case of *YS* channels set its two *LSBs* to zero but in case of *T* channel set three *LSBs* to zero.

3. In case of *T* channel, excluding the central four pixels of each 4×4 block, pass rest of the twelve neighboring pixels along with the ownership information like owner id, time stamp and private key to *SHA160*, hash function to compute the content based hash as shown in Fig. 1.

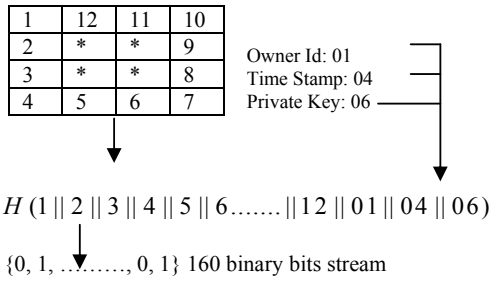


Fig.1 Content Based Hash Computation

4. Mapping of 160 bits stream to shorter and unique bits stream is important to control the payload of watermark. For instance a bit stream '1011' is mapped into '01' by applying *XOR* on 10 and 11, where 10 are the first two bits of hash bits stream and 11 are the last two bits of the hash bits stream. The mapping function is given by the equation (2).

$$m^x = \sum_{i=0}^{(160/r)-1} (b^x_{ir+1} \,||\, b^x_{ir+2} \,||\, \ldots\ldots\ldots \,||\, b^x_{ir+r}) \quad (2)$$

Where m^x, is the mapping function result and $\sum$ stands for logical *XOR* operator. The mapped bits will be finally inserted into LSBs of the corresponding block.

5. For recovery of work, intensity mean, of each channel's 4×4 block is computed.

6. For each channel, the mapping of blocks is done using equation (3) based on *2D Torus Automorphism* with the help of private key.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (3)$$

Where (x, y), $(x', y') \in [0, N-1] x [0, N-1]$, N is the number of blocks in each dimensions, and $k \in [0, N-1]$ is a private key.

7. In case of *T* channel, the watermark is formed by concatenating the hash bits and block intensity bits in a manner as shown in Fig. 2 and then embedded into the central 2×2 sub-block of each 4×4 block in a manner as shown in the Fig. 3.

h1	h2	h3	h4	i1	i2	i3	i4	i5	i6	i7	i8

Fig. 2 Generated Watermark Format for *T* channel

					LSB#3	LSB#2	LSB #1
					h1	i1	i2
					h2	i3	i4
					h3	i5	i6
					h4	i7	i8

Fig. 3 *T* Channel's 2×2 sub-block LSBs Structure

8. In case of *YS* channels, the watermark consists of only block intensity bits in a manner as shown in Fig. 4 and embedded into the central 2×2 sub-block of each 4×4 block in a manner as shown in Fig. 5.

i1	i2	i3	i4	i5	i6	i7	i8

Fig. 4 Generated Watermark Format for *YS* Channel

						LSB#2	LSB#1
						i1	i2
						i3	i4
						i5	i6
						i7	i8

Fig. 5 *YS* Channel's 2×2 sub-block LSBs Structure

9. After completing the embedding process, concatenate all the *Y, S* and *T* channels.

10. Transform the image from *YST* domain to *RGB* by taking inverse transform of equation (1) to have the watermarked image.

Watermark Extraction and Tamper Detection

1. Transform the given watermarked image from *RGB* to *YST* color space using equation (1) and select the *T* channel.

2. Using the same private key as used in embedding phase, generate the mapping sequence of non-overlapping 4×4 blocks of *T* channel using equation (3).

3. Extract only the hash bits, as indicated by symbol *LSB#3* in Fig. 3, from central 2×2 sub-block of each 4×4 block, for its correspondence source block.

4. After extraction of watermark, excluding the central 4 pixels, pass all the twelve neighboring pixels along with same ownership information to *SHA160,* hash function as shown in Fig. 1, to compute the one way hash bits and resize the hash bits in the same manner as done in embedding phase using equation (2).

5. Now compare the extracted and generated hash bits for the corresponding blocks, if they are same and equal in number, means image is authentic, otherwise tampered.

6. If the image is tampered, then identify that block and set its pixel value to zero.

Recovery of Tampered Work

1. Once the tamper detection is done correctly, identify the source block for the tampered block using the equation (3) with the same private key as used in embedding and tamper detection phase.

2. Generate the pixel value from the 8-bit watermark from the corresponding source block two *LSBs*, and set all the pixels of tampered block to this restored value.

3. Repeat step 1 and 2 for all the three channels.

4. Once the recovery is done, transform the image from *YST* to *RGB* color space by taking the inverse transform of equation (1).

IV. Results

The simulations were conducted on Intel machine with 2.4 GHz processor and 512 MB of RAM. MATLAB 7.0 and Photoshop 7.0 was used for implementation of proposed scheme and image processing operations.

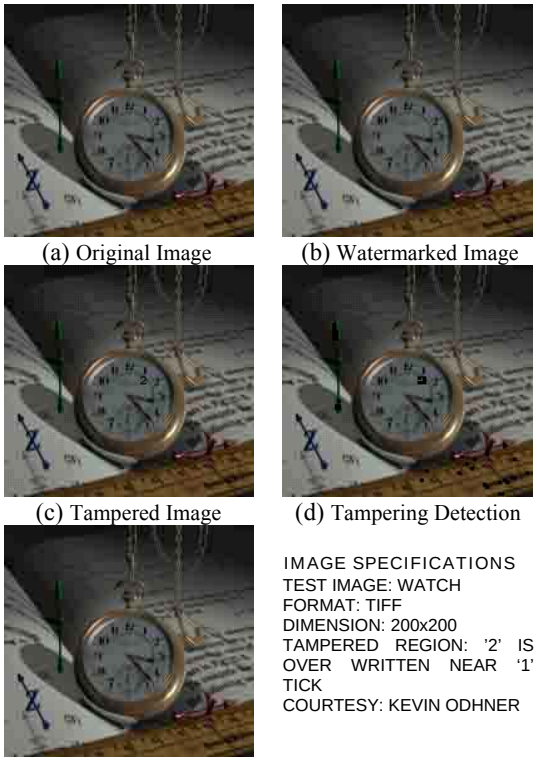
PSNR Measurement: One commonly used measure to evaluate the imperceptibility of the watermarked image is the peak signal to noise ratio *(PSNR)* which is given by the equation (4).

$$PSNR = 10.\log_{10}\left(\frac{255}{MSE}\right)(dB) \quad (4)$$

TABLE I
Quality Matrix (*PSNR*)

Image	Format	Size	PSNR (dB)
Lena	tiff	200x200	43.3654
Watch	tiff	200x200	43.3411
F16	tiff	200x200	42.8932
Baboon	tiff	200x200	43.1381
Opera	tiff	256x256	43.1213
Waterfall	tiff	256x256	43.1243

Table I shows the *PSNR* values computed for images used in our experiment for the implementation and verification of the proposed scheme.

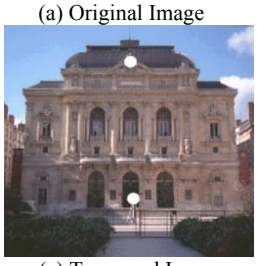


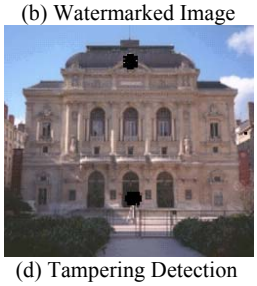
(a) Original Image (b) Watermarked Image
(c) Tampered Image (d) Tampering Detection
(e) Recovered Image

Fig. 6 Simulation Results: Watch


(a) Original Image


(b) Watermarked Image


(c) Tampered Image


(d) Tampering Detection

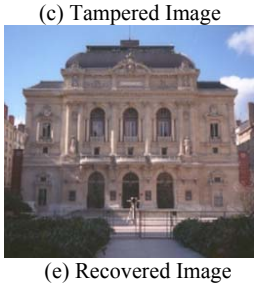
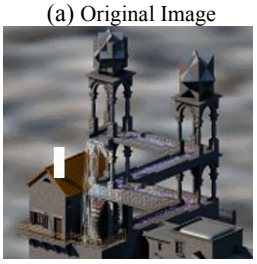

(e) Recovered Image

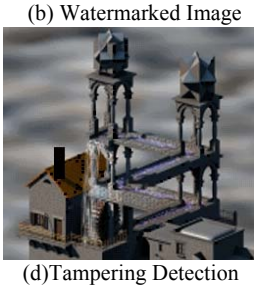
IMAGE SPECIFICATIONS
IMAGE: OPERA HOUSE OF LYON
FORMAT: TIFF
DIMENSION: 256x256
TAMPERED REGION: TOP and BOTTOM AREA OF HOUSE
COURTESY: F.A.P. PETITCOLAS

Fig. 7 Simulation Results: Opera House of Lyon


(a) Original Image


(b) Watermarked Image


(c) Tampered Image


(d)Tampering Detection

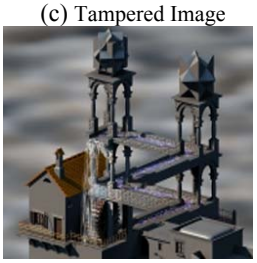

(e) Recovered Image

IMAGE SPECIFICATIONS
IMAGE: WATERFALL MODEL
FORMAT: TIFF
DIMENSION: 200x200
TAMPERED REGION: HOUSE FUNNEL
COURTESY: SASCHA LEDINSKY

Fig. 8 Simulation Results: Waterfall Model


(a) Original Image


(b) Watermarked Image


(c) Tampered Image


(d)Tamper Detection

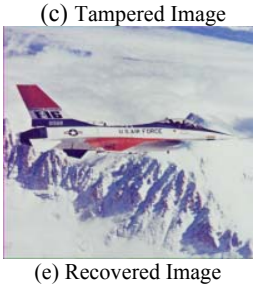

(e) Recovered Image

IMAGE SPECIFICATIONS
IMAGE: US F16
FORMAT: TIFF
DIMENSION: 200X200
COLORS BANDS: RGB
TAMPERED REGION: LOGO
COURTESY: UNIVERSITY OF SOUTHERN CALIFORNIA

Fig. 9 Simulation Results: US F16 Jet Plane

In Fig 6-9, caption (a), (b), (c), (d) and (e) of respective figure shows the original image, watermarked image, tampered image, detected image and recovered image respectively.

V. Concluding Remarks

In this paper, we proposed a scheme for *Ownership Identification* and *Color Image Authentication* with the ability to recover the original work. The proposed scheme deploys *Cryptography and Digital Watermarking* to have single solution for *Ownership Identification and Authentication.* The given color image that will proof the ownership is first transformed from *RGB to YST* color space, exclusively designed and recommended for watermarking based applications by Francesco et al. [2]. Followed by color space transformation, each channel is divided into 4×4 non-overlapping blocks and its central 2×2 sub-block is selected. In case of *YS* channels only two *LSBs* of each central 2×2 sub-block, are set to zero, to hold the recovery information but in case of *T* channel three *LSBs* of each central 2×2 sub-block are set to zero, to hold ownership information apart from recovery information. Geometrically $YS \perp T$ and therefore *T* gave us liberty to embed more bits. The size and position of sub-block is important for correct localization, enhanced security and fast computation. The 4×4 block of *T* channel along with ownership information is then deployed by *SHA160* to compute, content based hash that is unique and resistant against hash collision or birthday attack, identified by *RSA Data Security Inc and B. Schneier* [4]-[5] rather then

MD5 that may raise the condition i.e. $H(m) = H(m')$. For recovery, intensity mean of 4×4 block of each channel is computed with 8 bit intensity. The target block that will hold the source block information is determined by implementing *2D-Torus Automorphism* presented by G. Voyatzis et al. [6] using private key to have secure mapping of blocks. The perceptibility of watermarked image is quite reasonable in terms of *PSNR*. Our scheme is oblivious, correctly localizes the tampering in a work within reasonable time and with the ability to recover the original work of probability near one. In future we will investigate the proposed scheme under different attacks like vector quantization to check the degree of survival of our proposed scheme.

REFERENCES

[1] Chang C.C, Hu Y.S., Lu T.C. "A Watermarking-Based Image Ownership and Tampering Authentication Scheme", Elsevier, Pattern Recognition Letters, 2005.
[2] Francesco. B., Giunta. G., Neri. A. "A New Color Space Domain for Digital Watermarking in Multimedia Applications", IEEE Trans. Image Process, 2005.
[3] Maniccam, S.S., Bourbakis, N., "Lossless Compression and Information Hiding in Images, Pattern Recognition 37 (3), pp. 475–486, 2004.
[4] http://www.rsasecurity.com
[5] B. Schneier, Applied Cryptography, John Wiley & Sons, NY, 1996.
[6] G. Voyatzis, I. Pitas, "Applications of Toral Automorphism in Image Watermarking", ICIP, Vol II, 1996, pp.237-240, 1996.
[7] Lin, C.H., Hsieh, W.S., "Applying Projection and B-Spline to Image Authentication and Remedy", IEEE Trans. Consumer Electron. 49 (4), pp. 1234–1239, 2003.
[8] Lu, C.S., Liao, H.Y.M.,"Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme", IEEE Trans. Multimedia 5 (2), pp. 161–173, 2003.
[9] Barreto, P.S.L.M., Kim, H.Y., Rijmen, V., "Toward Secure Public-Key Blockwise Fragile Authentication Watermarking", IEE Proc. Vision, Image Signal Process. pp. 57–62, 2002.
[10] Celik, M.U., Sharma, G., Saber, E., Tekalp, A.M., "Hierarchical Watermarking for Secure Image Authentication with Localization, IEEE Trans. Image Process. 11 (6), pp. 585–595, 2002.
[11] Walton, S., "Information Authentication for a Slippery New Age", Dr. Dobbs Journal. 20 (4), pp. 18–26, 1995.
[12] Schyndel, R.G., Tirkel, A.Z., Osborne, C.F., "A Digital Watermark", Proceedings of the IEEE International Conference on Image Processing, Austin, Texas, vol. 2, pp. 86–90, 1994.
[13] Wolfgang, R.B., Delp, E.J., "A watermark for Digital Images", Proceedings of IEEE International Conference on Image Processing, Lausanne, Switzerland, vol. 3, pp. 219–222, 1996.

M. Hamad Hassan did his BS(CS) and MIT from Peshawar and Iqra University respectively. At present, he is HEC Scholar at Faculty of Computer Science & Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Pakistan for his MS in Computer System Engineering. He is also faculty member at the Institute of Information Technology, Kohat University of Science & Technology, Pakistan. His research interests include Digital Image Watermarking & Cryptography for Information Security.

Dr. Asif Gilani did his M.Sc from Islamia University Pakistan and Ph.D in Copyright Protection from University of Patras, Greece. He is Dean of Faculty of Computer Science & Engineering at Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Pakistan. His research interests include Digital Image Watermarking, Steganography and Image Authentication. He has published number of research papers internationally. At present he is supervising many MS/Ph.D students at GIK Institute. He is also at the list of HEC and PCST approved Ph.D supervisors.