World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:7, 2008

A Semi-Fragile Signature based Scheme for Ownership Identification and Color Image Authentication

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

***Abstract*—**In this paper, a novel scheme is proposed for ownership identification and authentication using color images by deploying *Cryptography and Digital Watermarking* as underlaying technologies. The former is used to compute the contents based hash and the latter to embed the watermark. The host image that will claim to be the rightful owner is first transformed from *RGB* to *YST* color space exclusively designed for watermarking based applications. Geometrically $YS \perp T$ and T channel corresponds to the chrominance component of color image, therefore suitable for embedding the watermark. The T channel is divided into 4×4 non-overlapping blocks. The size of block is important for enhanced localization, security and low computation. Each block along with ownership information is then deployed by *SHA160*, a one way hash function to compute the content based hash, which is always unique and resistant against birthday attack instead of using *MD5* that may raise the condition i.e. $H(m) = H(m')$. The watermark payload varies from block to block and computed by the variance factor α. The quality of watermarked images is quite high both subjectively and objectively. Our scheme is blind, computationally fast and exactly locates the tampered region.

***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 and 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. 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.

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

Dr. Asif Gilani is the Dean of Faculty of Computer Science and Engineering at GIK Institute, Pakistan (e-mail: 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

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 [11]-[13] which is twofold one 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 and can 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, we proposed a novel scheme for ownership identification and authentication of color images. The selection of color space is important as in *RGB* color space planes are highly correlated to each other therefore we deployed *YST* color space, exclusively designed for watermarking based applications recommended by Francesco et al. [2]. The given color image is first transformed from *RGB* color space to *YST* color space by using set of linear transformation matrix given by equation (1). Geometrically $YS \perp T$ and T channel corresponds to the chrominance component of color image and therefore recommended for embedding the watermark. The T channel is then divided into

non-overlapping blocks of size 4×4. The size of block is important for the improved localization and fast computation. Each block along with ownership information is then deployed by *SHA160*, one way hash function that generates the content based hash, which is unique and resistant to hash collision or birthday attack, as claimed by *RSA Data Security Inc. and B. Schneier* [6]-[7] rather than *MD5* that may raise the condition i.e. $H(m) = H(m')$.

The payload of watermark bits i.e. the bits to be embedded into each block central four pixels *LSBs* varies from block to block, and computed by the variance factor, α, that deploys all the twelve neighboring pixels as shown in the Fig. 2.The embedded watermark then votes for the ownership identification and authentication. Since only selected *LSBs* of central four pixels of each 4×4 block is deployed for watermark embedding, therefore our scheme is secure and produce watermarked images with high degree of imperceptibility in terms of *PSNR* with best localization of the tampered region.

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 [14] 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 operation 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. [15] 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 [16] 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 LSB's of the pixels that can be easily removed.

Chang C.C, Hu Y.S. and 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* [6]-[7], 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. 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) For the security perspective and avoid hash collision issues, *SHA160* is deployed, recommended by [6]-[7], that computes the hash, by deploying all the twelve neighboring pixels used for authentication and user desired information for ownership proof.

iv) The hash bits are embedded into the central four pixels *LSBs* rather than block's outside pixels *LSBs* so that one cannot remove them easily.

v) The length of hash bits i.e. watermark payload, is variable and dependent on the variance factor α computed from all the twelve neighboring pixels of each 4×4 block.

III. Roposed 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).

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

The *YST* color space can easily be related to all other color spaces, e.g. *YUV, YCbCr,* that are derived from the *RGB* image providing the calibration data. Geometrically $YS \perp T$ and $\theta = 52°$ between *YS*. The *T* channel is identified by the *Gram-Schmidt* approach and corresponds to the chrominance component of color image. For further details reader is recommended for paper presented by Francesco et al. [2].

Watermark Generation and Embedding

1. Select the *T* channel and divide it into 4×4 non-overlapping blocks.

2. Excluding the central four pixels, pass rest of the twelve neighboring pixels of block with user desired information like private key, time stamp, ownership id

etc. to *SHA160,* one way hash function to compute the content based hash as shown in the Fig. 1.

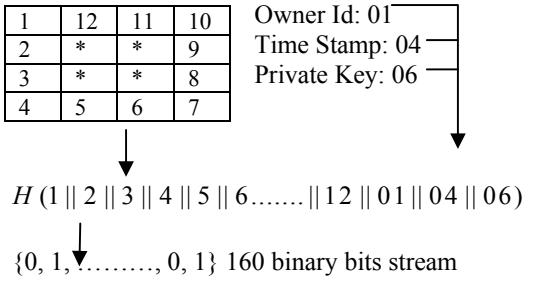


Fig. 1 Content Based Hash Computation

3. To determine the watermark payload, find the variance factor α as shown in the Fig. 2.

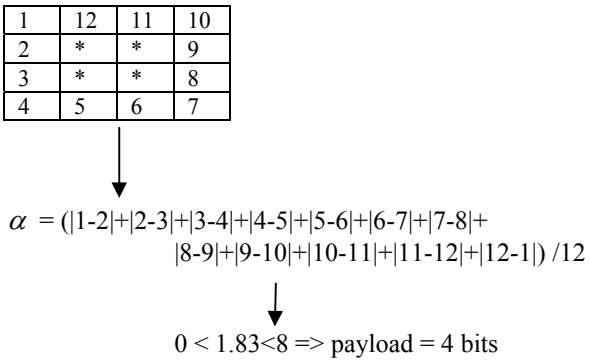


Fig. 2 Determining Watermark Payload

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).

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

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.

Authentication and Tamper Detection

Convert the given watermarked image, from *RGB* to *YST* color space and select the *T* channel. Divide the *T* channel into 4×4 non-overlapping blocks and extract the watermark bits from central pixels *LSBs*. The number of bits to be extracted is determined in the same way as shown in the Fig. 2 and using the equation (2). Then generate the hash of each block in the same way as done in watermark generation phase. After having both the extracted and generated watermark bits, compare them, if they are equal and same implies that image is authentic otherwise tampered. In case of tampering identify the block by setting its pixel values to zero.

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.

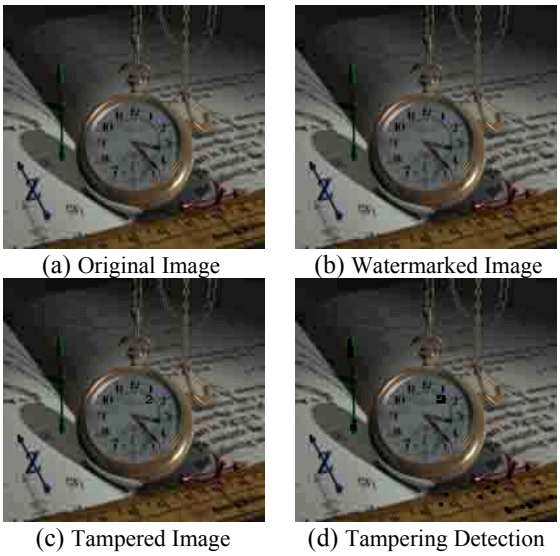
PSNR Measurement: One commonly used measure to evaluate the imperceptibility of the watermarked image is the peak signal to noise ratio *(PSNR)* which is given by the equation (3).

$$PSNR = 10.\log_{10}\left(\frac{255}{MSE}\right)(dB) \qquad (3)$$

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.

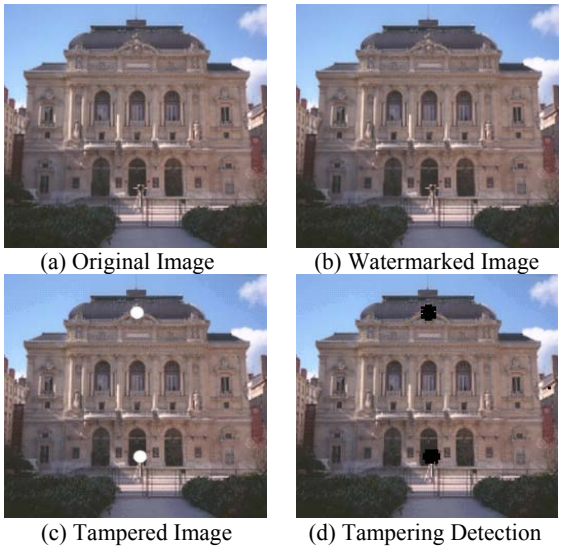


(a) Original Image (b) Watermarked Image

(c) Tampered Image (d) Tampering Detection

IMAGE SPECIFICATIONS
TEST IMAGE: WATCH
FORMAT: TIFF
DIMENSION: 200x200
TAMPERED REGION: '2' IS OVER WRITTEN NEAR '1' TICK
COURTESY: KEVIN ODHNER

Fig. 3 Simulation Results: Watch



(a) Original Image (b) Watermarked Image

(c) Tampered Image (d) Tampering Detection

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. 4 Simulation Results: Opera House of Lyon

In Fig. 3-4, caption (a), (b), (c) and (d) of the respective figure shows the original image, watermarked image, tampered image and detected image respectively.

V. Concluding Remarks

In this paper, we proposed a scheme for ownership identification and authentication using color images. The color image is first transformed from *RGB* to *YST* color space, exclusively designed for watermarking based applications. The *T* channel selected for embedding our watermark and divided into 4×4 non-overlapping blocks. The size of block is important for the sake of enhancing localization, security and fast computation. Each block along with ownership information is then deployed by *SHA160*, to compute the content based hash which satisfies $H(m) \neq H(m')$ always. The watermark payload is controlled by variance α by deploying all the twelve neighboring pixels. The embedded watermark then votes for the ownership identification and authentication. The *PSNR* value of our scheme watermarked image is quite optimistic. Our scheme has best localization property and exactly locates the tampered region; however it is challengeable for our scheme to recover the tampered work. We are still working on this issue and will be resolved soon.

References

[1] Chang C.C, Hu Y.S., Lu T.C., "A Watermarking-Based Image Ownership and Tampering Authentication Scheme", Elsevier, Pattern Recognition Letter, 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] Queluz, M.P, "Authentication of Digital Images and Video: Generic Models and a New Contribution", Signal Process: Image Comm. 16 (5), pp. 461–475, 2001.
[4] Maniccam, S.S., Bourbakis, N., "Lossless Image Compression and Encryption using Scan", Pattern Recognition 34 (6), pp. 1229–1245, 2001.
[5] Maniccam, S.S., Bourbakis, N., "Lossless Compression and Information Hiding in Images", Pattern Recognition 37 (3), pp. 475–486, 2004.
[6] http://www.rsasecurity.com
[7] B. Schneier, "Applied Cryptography", John Wiley and Sons, NY, 1996.
[8] 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.
[9] Lin, C.Y., Chang, S.F., "A Robust Image Authentication Method Distinguishing Jpeg Compression from Malicious Manipulation", IEEE Trans. Circ. Systems Video Technol. 11 (2), pp. 153–168, 2003.
[10] 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.
[11] Barreto, P.S.L.M., Kim, H.Y., Rijmen, V., "Toward Secure Public-Key Blockwise Fragile Authentication Watermarking", IEE Proc. Vision, Image Signal Process. 149 (2), pp. 57–62, 2002.
[12] 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.
[13] Chao, H.M., Hsu, C.M., Miaou, S.G., "A Data Hiding Technique with Authentication, Integration and Confidentiality for Electronic Patient Records", IEEE Trans. Inf. Technol. Biomed. 6 (1), pp. 46–53, 2002.
[14] Walton, S., "Information Authentication for a Slippery New Age", Dr. Dobbs J. 20 (4), pp. 18–26, 1995.
[15] 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.
[16] 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 and Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Pakistan for his MS in Computer System Engineering. He is also faculty member at the Institute of Information Technology, Kohat University of Science and Technology, Pakistan. His research interests include Digital Image Watermarking and 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 and Engineering at Ghulam Ishaq Khan Institute of Engineering Sciences and 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.