Multimed Tools Appl (2015) 74:7685–7709
DOI 10.1007/s11042-014-2006-2

Face region authentication and recovery system based on SPIHT and watermarking

Clara Cruz-Ramos · Mariko Nakano-Miyatake · Hector Perez-Meana · Rogelio Reyes-Reyes · Luis Rosales-Roldan

Received: 11 October 2013 / Revised: 18 February 2014 / Accepted: 4 April 2014 / Published online: 27 April 2014

Abstract The face regions of digital pictures are some of the principal target of tampering to generate a potential scandal, causing social and economic damages to involved persons. In this paper, we propose a face region authentication and recovery system, in which the face regions are automatically protected at the moment when the picture is taken by a digital camera. When the original face of the picture is replaced by another face by malicious person, the system can detect the tampered face and recover the original one. The proposed system consists of two stages: the face region protection stage and the face region tamper detection and recovery stage. In both stages, the face detection module based on the Viola-Jones algorithm, face region encoding/decoding modules based on the Set Partitioning in Hierarchical Trees (SPIHT) algorithm and watermarking module based on Quantization Index Modulation (QIM) are used. These three algorithms, Viola-Jones detector, SPIHT and QIM, are determined as most adequate algorithms for proposed system after several evaluations. The experimental results show a high quality of the watermarked as well as the recovered images, obtaining average Peak Signals to Noise Ratios (PSNR) of more than 40 and 38 dB, respectively.

Keywords Face detection · Tamper detection · Self-recovery · Watermarking · SPIHT · QIM

1 Introduction

Nowadays almost all newspapers offer their electronic versions in Internet, in which digital images have very important roll to provide news or articles. Also in social networks, many peoples publish their digital images together with some comments, because generally visual information given by images has more impact than the written information. However, digital images can be modified easily using computational tools, such as Photoshop and Corel Draw, without any visual artifact. In many cases, tampered images cause economic and social damages to the involved persons in the images. Considering the above situation, the

C. Cruz-Ramos · M. Nakano-Miyatake (✉) · H. Perez-Meana · R. Reyes-Reyes · L. Rosales-Roldan
Mechanical Electrical Engineering School, Instituto Politécnico Nacional, Av. Santa Ana no. 1000, Col. San Francisco Culhuacan, Mexico, DF, Mexico
e-mail: mnakano@ipn.mx

Watermarking-based Color Image Authentication With Detection And Recovery Capability

L. R. Roldan, M. C. Hernández, J. Chao, M. N. Miyatake and H. P. Meana

***Abstract*— In this paper a watermarking-based color image authentication with detection and recovery capability is proposed, in which a Halftone image is used as an approximated version of the luminance channel (Y) and a coded version of the coefficients of the Two Dimensional Discrete Cosine Transform of the chrominance channels (Cb, Cr) of the YCbCr color space are used as watermark signal. The luminance and chrominance information is embedded into the sub-bands of lowest frequency of the Integer Wavelet Transform of the original luminance channel using Quantization Index Modulation Dither Modulation. The luminance information in embedded into the LL sub-band meanwhile the chrominance information is embedded into the LH and HL sub-bands. Besides, a Multilayer Perceptron Neural Network is used as inverse halftoning to increase the quality of the recovered image. The experimental results show the effectiveness of the proposed method compared with some published before.**

***Keywords*— Watermark, Color Images, Authentication, Detection Capability, Recovery Capability, DCT, IWT, MLP.**

I. INTRODUCCIÓN

LA AUTENTICACIÓN y protección de imágenes digitales es de gran importancia para asegurar la propiedad intelectual. Una imagen digital es de fácil almacenamiento y transmisión, lo que representa una gran desventaja ya que es posible alterarla mediante programas de edición de imágenes provocando daños morales y/o económicos a las personas involucradas. Este problema puede ser resuelto mediante técnicas de marca de agua que permiten detectar y recuperar las áreas alteradas [1-4].

En [1], la imagen original es procesada mediante la Transformada Wavelet Discreta (DWT) para posteriormente aplicar la Transformada de Coseno Discreto (DCT) a la sub-banda LL de la DWT y crear la señal de marca de agua a partir primeros *m* coeficientes de frecuencias bajas de la DCT e insertarla en las sub-bandas LH y HL de la imagen original. En la etapa de autenticación y recuperación, la señal de marca de agua extraída se compara con la sub-banda LL de la DWT de la imagen recibida utilizando el Error Cuadrático Medio (MSE) y la imagen recuperada se obtiene a partir de la señal de marca de agua extraída. Los autores en [2], insertan dos señales de marca de agua en sub-bandas diferentes de la Transformada Entera Wavelet (IWT), una para autenticación y otra para recuperación. La señal de autenticación es una secuencia binaria pseudoaleatoria, mientras que la señal de recuperación es similar que en [1]. La señal de autenticación es extraída para detectar las áreas alteradas y recuperarlas utilizando la señal de recuperación. El método basado en Modulación de Índices por Cuantización usando Modulación Dither (QIM-DM) utilizando la IWT en [3] utiliza un patrón binario predefinido como señal de marca de agua de autenticación y una imagen halftone de la sub-banda LL generada por la segunda descomposición de la IWT como señal de marca de agua de recuperación. Este método muestra una gran robustez utilizando un valor de umbral adecuado, sin embargo este valor produce errores de falso negativo muy altos. En [4] una imagen halftone generada a partir de la primera descomposición de la IWT es insertada como señal de marca de agua en diferentes dominios espectrales (IWT o DCT) de la imagen original. En la etapa de autenticación las áreas alteradas son detectadas mediante el Índice de Similitud Estructural (SSIM) y recuperadas mediante la señal de marca de agua extraída mediante la implementación de una Red Neuronal Multicapas (MLP) como proceso inverso halftone. El principal problema de estos métodos [1]-[4], es que no han sido diseñados para imágenes a color por lo que no soportan ningún tipo de compresión.

En este artículo se propone un método de autenticación de imágenes a color basado en señales de marca de agua con capacidad de detección y recuperación de las áreas alteradas. La imagen original a color se convierte del espacio de color RGB al espacio de color YCbCr para crear una imagen halftone mediante el método propuesto por Floyd-Steinberg [5] del canal de luminancia (Y) y una versión codificada de los canales de crominancia (Cb y Cr) que serán utilizados como señales de marca de agua e insertadas mediante QIM-DM [6] en de la sub-banda LL de la primera descomposición de la IWT, y en las sub-bandas LL1 y LL2 obtenidas de la segunda descomposición de las sub-bandas HL y LH, respectivamente, del canal de luminancia (Y). En la etapa de autenticación se utiliza la imagen sospechosa (imagen marcada y posiblemente alterada) y la señal de marca de agua extraída para detectar las áreas alteradas mediante la Diferencia de Color Normalizada (NCD) y posteriormente recuperarlas mediante la señal de marca de agua extraída. En la etapa de recuperación se utiliza una MLP como proceso inverso halftoning a la información de la luminancia extraída para incrementar la calidad de la imagen recuperada.

El artículo esta ordenado de la siguiente manera. La sección II describe el método propuesto y los resultados

L. R. Roldan, Universidad de Chuo, Tokio, Japón, luis.rosales.roldan@gmail.com
M. C. Hernández, Instituto Politécnico Nacional, México D.F., México, mcedillohdz@hotmail.com
J. Chao, Universidad de Chuo, Tokio, Japón, jchao@ise.chuo-u.ac.jp
M. N. Miyatake, Instituto Politécnico Nacional, México D.F., México, mnakano@ipn.mx
H. P. Meana, Instituto Politécnico Nacional, México D.F., México, hmperezm@ipn.mx

Multimed Tools Appl (2018) 77:16031–16052
DOI 10.1007/s11042-017-5178-8

Color image ownership protection based on spectral domain watermarking using QR codes and QIM

Luis Rosales-Roldan[1] · Jinhui Chao[2] · Mariko Nakano-Miyatake[3] · Hector Perez-Meana[3]

Received: 30 October 2016 / Revised: 18 August 2017 / Accepted: 30 August 2017 /
Published online: 9 September 2017

Abstract Some watermarking authentication methods based on spectral domain using QR codes and Quantization Index Modulation (QIM) are proposed for ownership protection in color images. The QR code is created with the owners' information and used as binary watermark sequence, which is permuted using Arnold Permutation to increase the security before embedding it. Once the watermark sequence is generated, the original color image is transformed from RGB to YCbCr color space where the Luminance Channel (Y) is processed by the Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) to embed the binary watermark sequence using Quantization Index Modulation (QIM). The experimental results show the effectiveness of the proposed method.

Keywords Watermarking · QIM · QR code · Ownership · Color Images · SVD/DWT/DCT

1 Introduction

Due to the easy transmission of digital multimedia, the shared information is always vulnerable to unauthorized access and then, an effective way to protect the digital multimedia is necessary. At the same time, watermarking technics are very effective to hide information into an image providing high imperceptibility, robustness and security. The proposed methods [1, 7, 8, 12,

✉ Luis Rosales-Roldan
luis.rosales@upaep.mx; luis.rosales.roldan@gmail.com

[1] Department of Mechatronics, Universidad Popular Autónoma del Estado de Puebla, 17 Sur 901, Barrio de Santiago, Puebla, Mexico

[2] Department of Information Engineering, Faculty of Science and Technology, Chuo University, Tokyo, Japan

[3] Graduate Section, Mechanical Electrical Engineering School, Instituto Politécnico Nacional, Mexico, Mexico

Signal Processing: *Image Communication* 28 (2013) 69–83

Contents lists available at SciVerse ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

Watermarking-based image authentication with recovery capability using halftoning technique

Luis Rosales-Roldan [a], Manuel Cedillo-Hernandez [b], Mariko Nakano-Miyatake [a,*], Hector Perez-Meana [a], Brian Kurkoski [c]

[a] *Postgraduate Section, Mechanical Electrical Engineering School, National Polytechnic Institute of Mexico, , Mexico*
[b] *Electrical Engineering Division, Engineering Faculty, National Autonomous University of Mexico, Mexico*
[c] *Japan Advanced Institute of Science and Technology, Japan*

ARTICLE INFO

Article history:
Received 13 November 2011
Accepted 15 November 2012
Available online 23 November 2012

Keywords:
Watermarking
Content authentication
Recovery capability
Halftoning
IWT
DCT
SSIM criterion

ABSTRACT

In this paper two watermarking algorithms for image content authentication with localization and recovery capability of the tampered regions are proposed. In both algorithms, a halftone version of the original gray-scale image is used as an approximated version of the host image (image digest) which is then embedded as a watermark sequence into given transform domains of the host image. In the first algorithm, the Integer Wavelet Transform (IWT) is used for watermark embedding which is denominated WIA-IWT (Watermarking-based Image Authentication using IWT), while in the second one, the Discrete Cosine Transform (DCT) domain is used for this purpose, we call this algorithm WIA-DCT (Watermarking-based Image Authentication using DCT). In the authentication stage the tampered regions are detected using the Structural Similarity index (SSIM) criterion, which are then recovered using the extracted halftone image. In the recovery stage, a Multilayer Perceptron (MLP) neural network is used to carry out an inverse halftoning process to improve the recovered image quality. The experimental results demonstrate the robustness of both algorithms against content preserved modifications, such as JPEG compression, as well as an effective authentication and recovery capability. Also the proposed algorithms are compared with some previously proposed content authentication algorithms with recovery capability to show the better performance of the proposed algorithms.

1. Introduction

Nowadays the developments based on digital technology have a strong impact on the people's life, for example it is quite common to take pictures everywhere and every time using his/her cellular phones with digital cameras, giving as a results that about 700,000 pictures per hour are uploaded to any computer network to be shared among different users. This kind of images can be easily manipulated, realizing for example copy-and-paste operations, in which some part of the image is replaced by a part of another or the same image. These manipulations can be done using simple tools available in any PC, such as Photoshop and Corel Draw, etc., without almost any perceptual distortions. However, sometimes these alterations cause economical and/or moral damages to involved persons. This is one of the main reasons why digital image authentication has become one of the most important issues in the information security fields.

Cryptographic approaches, such as cryptographic hashing [1] and fragile watermarking [2–10] are effective digital material authentication methods. Almost all fragile

* Corresponding author.
E-mail address: mariko@infinitum.com.mx (M. Nakano-Miyatake).

0923-5965/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.image.2012.11.006