International Journal of Electronics Engineering, 2(1), 2010, pp. 1-3

A New Cryptography Based Watermarking Technique for Information Security

Ajay Goel[1], O. P. Sahu[2], Sheifali Gupta[3] & Rupesh Gupta[4]

[1]*Department of Computer Sc.& Engg., Singhania University, Jhunjhunu (Rajasthan), INDIA*
[2]*Department of Electronics and Communication Engineering, NIT (Kurukshetra), INDIA*
[3]*Department of Electronics Engg., Singhania University, Jhunjhunu (Rajasthan), INDIA*
[4]*Department of Mechanical Engg. , Singhania University, Jhunjhunu (Rajasthan), INDIA*

Abstract: The growth of networked multimedia systems has created a need for the copyright protection of digital images and video. Copyright protection involves the authentication of image content and/or ownership. One approach is to mark an image by adding an invisible structure known as a digital watermark to the image. Digital watermark is a pattern of bits inserted into an image, audio or video file, which contains information related to this file. The purpose of digital watermark is to provide copyright protection for intellectual property that is in digital format. The signature or watermark is hidden such that it's perceptually and statistically undetectable. Then this signature or watermark can be extracted from the host media and used to identify the owner of the media [2].In this paper we will introduce a new algorithm of embedding the watermark in the host image with signature.

Keywords: Image Watermarking, Copyright Protection, Watermarking Techniques, Digital Watermarking, Steganography, Digital Signature

1. INTRODUCTION

Digital document can be distributed via the World Wide Web to a large number of people in a cost–effective way, but the increasing importance of digital media brings a new challenges as it now straightforward duplicate and even manipulate multimedia content this give a strong need for security services in order to keep the distribution of digital multimedia work both profitable for the document owner and reliable for the customer. Digital data can easily be exactly copied; this very useful but it also poses problems such as detect their values, for example, digital images, or record music digital, replacing a given piece of digital data cannot be distinguished and their pedigree cannot be confirmed. It's impossible to determine which piece is the original and which is the copy. The legality of defeating such techniques is debatable but the weakness of the technical approach is not [1].

2. DIFFERENT TYPES OF WATERMARKS

Some of the different types of watermarks that have been developed in the past few years are listed below:

2.1. Visible Watermarks

Are designed to be easily perceived by the viewer, and clearly identify the owner; the watermark must not detract from the image content itself, however.

*Corresponding Author: [1]goelajay1@gmail.com, [2]ops_nitk@yahoo.co.in, [3]sheifali@yahoo.com, [4]rup_esh100@yahoo.co.in

2.2. A Watermark May be Fragile, Semi-fragile or Robust

Fragile watermarks are designed to be distorted or "broken" under the slightest changes to the image. Semi-fragile watermarks are designed to break under all changes that exceed a user-specified threshold. [A threshold of zero would form a fragile watermark.] Robust watermarks withstand moderate to severe signal processing attacks (compression, rescaling, etc.) on an image.

2.3. Spatial Watermarks

Are constructed in the image spatial domain, and embedded directly into an image's pixel data. Spectral (or transform-based) watermarks are incorporated into an image's transform coefficients (DCT, Wavelet).

3. WATERMARKING PRINCIPLE

There are some of the steps that are required to embed some digital data in host image to create a watermark image these steps consist of [1]:

1. Generating the mark.
2. Embedding the mark.
3. Creating the key file.
4. Producing watermarked image.

Figure. 1: Show Both the Encoding and Decoding Process.

The encode process is consist of reading the host image (H) and using mark image (W) to generate the watermark image (HW).The encode process is used to extract the mark image from the watermark image by using the keyfile (Key).

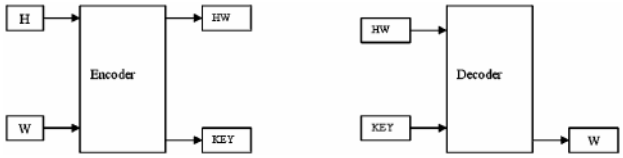

Figure 1: The Steps Used in Watermark Process.

To be really effective for copyright enforcement, a digital watermarking technique must satisfy the following requirements [2]:

3.1. Perceptual Transparency

The watermark must be embedded without affecting the perceptual quality of the host media under typical perceptual conditions. That is, human observers cannot distinguish the original host media from the watermarked media.

3.2. Unambiguity

The retrieval of watermark should unambiguously identify the owner. In addition, the accuracy of owner identification should degrade gracefully under attacks.

As a watermark is used to identify the owner of digital media, removal of the embedded watermark should be difficult for an attacker or any unauthorized user.

3.3. Tamper -Resistance

The embedded watermark must be resistant to tampering through collusion by comparing multiple copies of the media embedded with different watermarks.

4. THE PROPOSED ALGORITHM OF THE WATERMARKING TECHNIQUE

The embedded watermark must be invisible to human eyes and robust to most image processing operations. To meet these requirements, a bit of binary pixel value (0 or 1) is embedded in block of the host image. Before insertion, the host image is decomposed into NxN blocks.

The sizes of the host and watermark determine the size of the blocks, so in this paper the size of the host image is 512x512 pixel grayscale images with intensity values between 0 and 255 and the watermark is a 128x128 binary image, so the bits for the watermark are embedded into 4x4 blocks (B) of the host image. The algorithm of embedded a signature in the host image need to divide the algorithm in two categories:

4.1. Watermark Embedding

After dividing the host image into 4x4 blocks, the steps of insert the bits of the watermark image into each block (B) in the host image are [2]:

1. Compute the average, g_{mean}, minimum, g_{min}, and maximum, g_{max}, of the intensities on the pixels in *B*.
2. Classify each pixel into one of two categories, based on whether its intensity value is above or below the mean of the block. i.e., the ijth pixel, *bij* is classified depending on its intensity, g, as: $b_{ij} \in Z_H$ if $g > g_{mean}$ *bij* € *ZL* if $g \le g$ mean Where: Z_H and Z_L are the high and low intensity classes, respectively.
3. Compute the means, m_L and m_H, for the two classes, Z_L and Z_H.
4. Define the contrast value of block *B* as

$$C_B = \max (C_{min}, \alpha (g_{max} - g_{min}))$$

Where: a. α is a constant.

b. C_{min} is a constant which defines the minimal value a pixel's intensity can be modified.

5. Given the value of the signature image b_w is 0 or 1, modify the pixels in *B* according to:

   If $b_w = 1$, $g_{new} = g_{max}$ if $g > m_H g_{new} = g_{mean}$ if $m_L \le g < g_{mean} g_{new} = g + \delta$ otherwise

   If $b_W = 0$, $g_{new} = g_{min}$ if $g < m_L g_{new} = g_{mean}$ if $g_{mean} \le g < m_H g_{new} = g - \delta$ otherwise

   Where g_{new} is the new intensity value for the pixel which had original intensity *g* value and δ is a random value between 0 and C_B.
6. The modified block of pixels, B_{new}, is then positioned in the watermark image in the same location as the block, *B*, of pixels from the original host image.

These steps describe the procedure by which the watermarked image is generated from a host and a watermark. The pixel intensities are modified within a range specified by the contrast value for a given block. If the contrast value is large, then the pixels are modified more than if the contrast value is small. Thus, the pixels are modified in a manner that is adaptive to the contrast value of the regional block of pixels. The result is that, if a 1 is embedded into a block, the average intensity value for that embedded block will be greater than the average intensity for the same block of the original host image. If a 0 is embedded, then the average intensity of the embedded block will be lower than that of the original host. By using the offset δ, those pixels which it modifies will have a small

random noise component, however with a nonzero overall mean value. The filtering that might be performed on the watermarked image may reduce the variance of the noise[7].

4.2. Extracting the Embedded Watermark:

The extraction algorithm is straightforward and requires retrieving the original host image. The extractor need only compute the sum of the intensity values for the block of the host and watermarked image. A bit is decoded by making the comparison of the two resultant values [2]: If $S_W > S_o$, then $b_W = 1$ If $S_W \leq S_o$, then $b_W = 0$

Where S_W and S_o, are the sums for the blocks of the watermarked and original images respectively. The decoded bits are then entered into the inverse permuted order as the NXN blocks were selected by using the key from the scrambled insertion procedure. This produces the recovered scrambled watermark. Then, the scrambled watermark is descrambled according to the key from the initial scrambling operation.

5. EXPERIMENTAL RESULTS

Figure 2: The Host Image and the Signature Image.

Figure 3: The Watermarked Image.

The experimental results are introduced in this section by using host image with size 512x512 and signature image with size 128x128. Figure (2) show the original host image and signature image. Figure (3) show the watermark image and it can be that there is no visible deference between the original host image and the watermark image.

6. CONCLUSION

From the experimental results some of points can be derived:

1. There is no visible deference between the original host image and the watermark image.
2. The sizes of the host and signature images must be compatible in order to insert the bits of the signature on the blocks of the host images.

REFERENCES

[1] V. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", *in Proceedings of the 3rd International IEEE Conference on Industrial Informatics*, Perth, Western Australia, 10-12 Aug 2005.

[2] Chang-Hsing Lee and Yeuan-Kuen Lee, "An Adaptive Digital Image Watermarking Technique for Copyright Protection", *IEEE Transactions on Consumer Electronics*, **45**, November 1999.

[3] P. Meerwald, "Digital Image Watermarking in the Wavelet Transform Domain Master's Thesis", *Department of Scientific Computing*, University of Salzburg, Austria, January 11, 2001.

[4] H. Guo and N. Georganas, "Digital Image Watermarking for Joint Ownership Verification without a Trusted Dealer", *proc. IEEE CME2003*, Baltimore, MD, USA, June 2003.

[5] J.K. O'Ruanaidh and T. Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking ", *IEEE International Conference on Image Processing*, October 26-29,. 1997. pp. 536-539.

[6] A. Wakatani, "Digital Watermarking for ROI Medical Images by Using Compressed Signature Image", *Faculty of Science and Engineering*, Konan University, Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

[7] Maha Mehde, "A Digital Image Watermarking Technique for Copyright Protection", *et al. Transaction Security System, in I.B.M. Systems Journal*, **30**, No. 2, pp 206-229, 1991.