

Composite Signature Based Watermarking for Fingerprint Authentication

Farid Ahmed
Department of EECS
The Catholic University of America
Washington, DC 20064, USA
1-202-319-5019
ahmed@cua.edu

Ira S. Moskowitz
Center for High Assurance Computer Systems
Naval Research Laboratory
Washington, DC 20375

moskowitz@itd.nrl.navy.mil

ABSTRACT

Digital watermarking is a technology to hide information in digital media. We extend the digital watermarking technique Phasemark™, originally developed solely for image authentication, to biometrics to assist in forensic analysis. Using a signature extracted from the Fourier phase of the original image, we hide an encoded signature back into the original image forming a watermarked image. The hiding occurs in the Fourier transform frequency domain. The detection process computes the Fourier transform of the watermarked images, extracts the embedded signature and then correlates it with a calculated signature. Various correlation metrics determine the identity degree of biometric authentication. We show how a composite filter can be used in conjunction with Phasemark™ for robust authentication of fingerprints.

Keywords

Phasemark™, biometric authentication, fingerprint, watermarking, composite filter, phase only filter.

1. INTRODUCTION

With the widespread infusion of digital technologies, and the proportional ease of distribution of digital contents over the internet, digital rights management (DRM) has become an issue of critical concern. The requirements of DRM often are encapsulated in three different aspects of the computer and network assurance literature [1]. These are confidentiality of communication, integrity of contents, and access control or authentication. Confidentiality and integrity of contents have traditionally been addressed by cryptographic security protocols, while access control or authenticity verification has been addressed by both

cryptographic, and non-cryptographic solutions such as digital watermarking [2], as well as by biometric authentication [3,4].

Biometric authentication refers to the verification of individuals based upon their physiological and behavioral characteristics such as fingerprint, face, iris, hand geometry, keystroke, voice, and retina identification [5-6]. Although, the acceptance and use of biometric authentication has had a slow go of it, biometric technology presently is close to maturity and is increasingly being accepted as a tool for identification and authentication [3]. Fingerprint biometrics specifically has been shown to have high effectiveness in terms of distinctiveness, permanence, and performance [6]. This is the first motivation for our paper. In particular, we show how modifications and improvements of our novel semi-robust watermarking technique Phasemark™ [7] can be used as a biometric tool for fingerprint authentication. Note, a strength of our method is that it is a *self-authentication* method, and the authentication information is carried as an integral part of the fingerprint image. Other methods may use meta-data, or an external database of fingerprint signatures to perform the authentication. In this short paper we do not do a comparison with other methods.

A motivation for the use of watermarks in biometric systems has been the need to provide increased security to the biometrics themselves and to this end, there have been some accomplishments, *e.g.*, [5-6, 8-9]. We propose to use a composite signature based watermarking technique, based upon our previous work Phasemark™, for robust fingerprint authentication, when dealing with variants of the same fingerprint. In particular, to make the authentication robust to the natural variations of different impressions of the same fingerprint, we use the notion of a training based composite filter [10-11].

2. SIGNATURE-BASED WATERMARK

2.1 Phasemark™

Let h represent a grayscale image that we wish to watermark. All processing starts on h after it has been realized in the spatial domain. We only consider compressionless TIFF, so no information is lost when going from the TIFF file format to the spatial representation as an eight bit grayscale image and back

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MM & Sec '05, August 1-2, 2005, NY, NY, USA.

Copyright 2005 ACM 1-59593-032-9/05/0008...\$5.00.

again to the TIFF file format (unless the image has been modified in some other manner). Note that our results are not limited to TIFF, any uncompressed image format will work, however for simplicity we use the term TIFF in this paper.

PhasemarkTM was first described in [7]. PhasemarkTM is a semi-robust Fourier domain authentication watermark for images. PhasemarkTM has been shown to be robust to various image formats [7] and has been modified to work in the wavelet domain [15]. We use the initial Fourier domain approach in this paper. As stated, for the sake of simplicity in this paper we use a grayscale TIFF image h . To signify the spatial coordinates of h we will write $h(m,n)$. The watermark of h is formed from a signature of the image, taken in the Fourier frequency domain. To be specific we apply the discrete Fourier transform (DFT) to h and get H . That is $H(u,v) = X(u,v) \exp(j\phi(u,v))$, where the complex number $H(u,v)$ is the (u,v) -th (Fourier) frequency, $X(u,v)$ is the (Fourier) magnitude $|H(u,v)|$, j is the principal square root of -1 , and $\phi(u,v)$ is the phase of $H(u,v)$ (values are in $(-\pi, \pi]$). The real valued $X(u,v)$ is rounded to the nearest integer and expressed as $R(u,v)$. The rounded values R can be expressed in bit slice format as $R=R_{q-1}, R_{q-2}, \dots, R_1, R_0$, where R_i is the i^{th} bit-plane of the rounded magnitude. We pick a specific value of i and modify R_i . Before we modify R_i we apply a filter $b(u,v)$ to $H(u,v)$ as follows:

$$b(u,v) = +1, \text{ if } \cos(\phi(u,v)) \geq 0 \\ = -1, \text{ otherwise} \quad [1]$$

This has the effect of clamping the phase angles at either 0 or π radians. We filter the phase angles one more time by mapping the $b(u,v)$ values $+1(-1)$ to $+1(0)$, respectively. This forms the binary phase only filter (BPOF) $B(u,v)$, which is the signature that we hide in the original cover image h . Using a non-avalanche (small processing errors do not grossly affect the correlation) type cipher we encrypt $B(u,v)$ (symmetric key) resulting a bit plane $E(B(u,v))$. We replace R_i with $E(B(u,v))$, which results in a modified Fourier magnitude $X(u,v)'$. We apply the inverse discrete Fourier transform (IDFT) to $X(u,v)' \exp(j\phi(u,v))$, which results in our modified image h' . We save this file as an (uncompressed) TIFF file. We freely interchange spatial realization and the TIFF file in this paper. h' is the watermarked image. We note that changing the magnitude of a complex number does not change its phase angle. Therefore, the only difference between the phases of h and the phases of h' come about from the rounding done to the spatial pixel values (by clipping and clamping), not to the bit plane replacement. We use PhasemarkTM for two detection correlation tests. In both tests, we assume that the detector has knowledge of the symmetric watermarking key. Before we discuss these two tests we discuss how PhasemarkTM is used to determine if an image is watermarked according to the PhasemarkTM algorithm (we say that such an image is *Phasemarked*), we call this the *basic correlation test*.

The basic correlation test is developed in [7]. Given a test image t , we determine if t is Phasemarked. Apply the DFT to t , $\text{DFT}(t) = T$. We extract R_i from T as above. We apply the decryption algorithm using the symmetric key, extract the hidden phase

signature from T , if T is in fact watermarked. If T is not watermarked, then this extraction process should not give us the hidden signature, it gives us garbage. We verify this by a correlation test. We denote the candidate extracted signature (binary phase only filter) [13] information as $B'(u,v)$. To perform the correlation test we map B' to $\{1,-1\}$ by sending $+1(0)$ to $+1(-1)$. We denote this renormalized candidate hidden phase information as b' . We apply a phase only filter to the frequency representation of our test image T . That is since

$$T(u,v) = T(u,v) | \exp(j\phi_T(u,v)) \quad [2]$$

we use phase only filter $T_{POF}(u,v) = \exp(-j\phi_T(u,v))$. This results in values on unit circle the complex plane. These values are gauged against the candidate hidden signature b' (see [7] for details) by term by term multiplication. We then apply the IDFT to this matrix which results in our correlation values. The basic correlation test is not used in this paper; since our concern is not if an image is Phasemarked, rather our concern is does our fingerprint signature match what the image is telling us.

2.2 Composite Signature

The first test we perform is the *signature-authentication test*. In this, we have a generic signature, which may or may not be derived from the BPOF of the image C in question. However, this signature is put into C via the PhasemarkTM method of replacing the i -th bit plane of the Fourier magnitude with the encrypted version of the signature. The resultant image is C' . Now we run the PhasemarkTM correlation detector just as in the basic correlation test. That is, we extract the signature from C' and correlate it against the pof from C' . Of course, if the signature is the BPOF of C' then we are in the identical situation as in the basic correlation test. However, in the signature-authentication test we allow for more general types of signatures that enable us to "hide" more than simply the BPOF of an image back in itself. In particular, in this paper we hide a composition of BPOFs. That is, given a training set of images T_i , we have the Fourier phase $\phi_i(u,v)$ of each image. We then compute $b_i(u,v)$ of each image as before (Eq. (1)). From this we use a *majority rule algorithm* [14] and define the *composite signature* at frequency (u,v) by

$$B_{comp}(u,v) = +1, \text{ if } \sum b_i(u,v) \geq 0 \\ = -1, \text{ otherwise} \quad [3]$$

The second test we perform using PhasemarkTM is the *marked/unmarked test*. In this test, we take a known marked image A and compare it to an unmarked image C . If C and A are "similar" this test should result in high correlation values. In detail, we extract the hidden signature from A using the watermarking key and correlate it against the pof from C .

Therefore, we see that PhasemarkTM can be generalized by using composite signatures and different correlation tests.

embed the composite signature into the first group of eight forming 101_1',..., 101_8'.

6. This is similar to Test 4, except that the composite signature is formed from 101_1, 101_2, 101_3, and 101_4. and we embed the composite signature into the first group of eight forming 101_1',..., 101_8'.
7. This is similar to Test 4, except that the composite signature is formed from 101_1, 101_2, 101_3, 101_4, 101_5 and 101_6. and we embed the composite signature into the first group of eight forming 101_1',..., 101_8'.

Note that tests 5-7 are variations of test 4, where they differ in the number of fingerprint impressions used in computing the composite signature. Therefore, we are not displaying the partial correlation distribution as in Figure 4. Instead, Table 2 enumerates the difference in (PACE) detection performance. For example, Test 5 uses the first two impressions and consequently correlation statistics for these two are significantly higher than all others. Similar observation can be made for Test 6 and 7 results (column 3 and 4 from Table 2).

Table 2. Detection performance with different composite signature

Test4 Compo 8	Test5 Compo 2	Test6 Compo 4	Test7 Compo 6
33	39.1	36.4	34.5
33.3	39	36.4	34.9
33.4	13.6	36.1	34.5
33	13.2	36.2	34.5
32.9	14.3	13	34.4
33.2	13.7	13.6	34.6
33.3	13.4	13.4	12.9
33	15.4	13.3	13.2
13.4	14.7	13.8	13.5
13.8	14.1	12.8	12.7
13.1	14.2	13.8	13.4
13.5	13.8	13.3	13.2
13.6	13.2	13.5	13
14.3	13.1	13.2	12.8
14.6	13.4	12.9	13
13.6	14.2	13.9	15.7

Let us now see closely the contribution of composite signature in this authentication scheme. Here we focus on the two tests done in test 3 (without composite signature) and 4 (with composite signature). Figure 5 and 6 show the PACE value distribution of all 6400 correlation tests done in tests 3 and 4 respectively. Figure 5 demonstrates the histogram of correlation values, when no composite signature is used. Note that there is even overlap of correlation values coming out of forged and

authentic fingerprints. By forged, we mean that the fingerprint was not part of the signature generation process. Of course a fingerprint is considered authentic if it used to form the signature (composite or non-composite). Figure 6 shows the corresponding results with the composite signature. The separation between the distributions for forged and authentic is now very clear. This can be used to choose a threshold for fingerprint authentication, as demonstrated by Figure 7 Receiver Operating Characteristics (ROC). Note AAR is authentic acceptance ratio, and FAR is false acceptance ratio (see [9]).

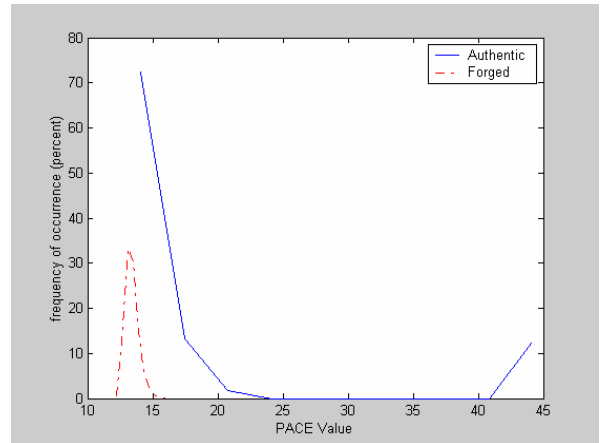


Figure 5. Histogram of detection metric with no composite signature (Test 3)

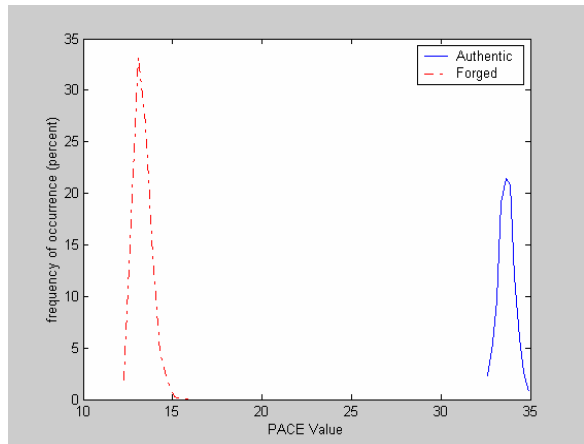


Figure 6. Histogram of detection metric with composite signature (Test 4)

