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

A Robust Image Watermarking Scheme using Image Moment Normalization

Latha Parameswaran, and K. Anbumani

***Abstract*—**Multimedia security is an incredibly significant area of concern. A number of papers on robust digital watermarking have been presented, but there are no standards that have been defined so far. Thus multimedia security is still a posing problem. The aim of this paper is to design a robust image-watermarking scheme, which can withstand a different set of attacks. The proposed scheme provides a robust solution integrating image moment normalization, content dependent watermark and discrete wavelet transformation. Moment normalization is useful to recover the watermark even in case of geometrical attacks. Content dependent watermarks are a powerful means of authentication as the data is watermarked with its own features. Discrete wavelet transforms have been used as they describe image features in a better manner. The proposed scheme finds its place in validating identification cards and financial instruments.

***Keywords*—**Watermarking, moments, wavelets, content-based, benchmarking.

I. Introduction

DIGITAL watermarking is defined as the process of embedding data (watermark) into a multimedia object to protect the owner's right to that object...

Digital watermarks have three major application areas: data monitoring, copyright protection and data authentication. There are several types of watermarking systems categorized based on their inputs and outputs [4]: *private watermarking and semi-Private watermarking. Public watermarking* is the most challenging scheme, as it requires neither the source image nor the watermark. These systems extract exactly a set of bits of information (namely the watermark) from the watermarked image. These schemes are also called *blind* watermarking. Another scheme is a*symmetric watermarking* which has the property that any user can read the watermark, without being able to remove it. Figure 1 shows a general watermarking scheme, cover image *I*, a watermark *W,* secret key *K*, and a watermarked image *I*.*

Manuscript received March 31, 2005.

Latha Parameswaran is with Amrita Deemed University, Coimbatore, India (91-11-2656422, p_latha@ettimadai.amrita.edu).

K. Anbumani is with Karunya Deemed University, Coimbatore, India (91-11-2646522, anbumani_k@yahoo.co.uk).

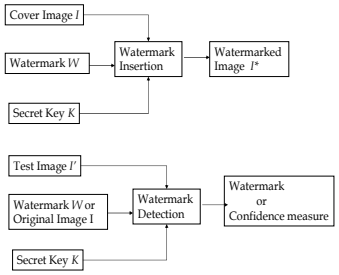


Fig. 1 General Watermarking Scheme: Insertion and Detection

Attacks on multimedia data can be roughly categorized into four classes [1]: Removal attacks such as lossy compression (JPEG), filtering, denoising and sharpening; Geometrical attacks such as warping and jitter; Protocol attacks such as copy attack and watermark inversion; Cryptographic attacks such as key search and oracle attacks. Of all these, removal attacks are less challenging and easy to handle. Geometrical attacks are a serious problem and there are not many techniques that have handled this attack. In [2] [6] the authors have presented a Rotation, Scaling and Translation resilient watermarking scheme based on Fourier-Mellin transform. Image moment normalization has been proposed to recover geometrical transformations [3]. The major drawback is that, it does not preserve image fidelity but creates contrast variations in the watermark image and cannot tolerate changes in aspect ratio and cropping. The scheme discussed in this paper is a blind (public) watermarking scheme, which does not require either the source image or the watermark to detect the presence of a watermark. The proposed watermarking scheme is divided into three major components: (1) Image Normalization (2) Content-Dependent watermark generation and (3) Watermark Embedding and Detection.

II. The Proposed Image Watermarking Scheme

The embedded watermark is a message that is encrypted using a secret key known to the sender and receiver. The message to be hidden is the details of the contract between the seller and buyer. Fig. 2 depicts the proposed image-watermarking scheme.

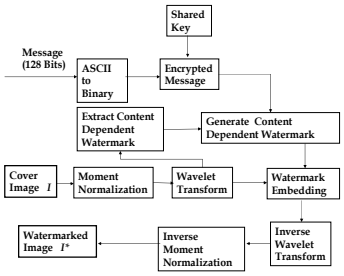


Fig. 2 Proposed watermarking scheme

A. Composing the Message to Hide

The message to be hidden is composed based on the buyer and seller information. The message is a binary text consisting of details as Seller identification (Name of Seller or any other information), Buyer identification (Name of Buyer or any other information), Key for encryption, Date of transaction, Sale contract details and any other relevant data. This data is converted to a binary string of 128 bits (or more as desired). This information forms the message to be hidden in the source image. Let this message be denoted as *M*.

B. Encrypting the Message to Hide

A key is chosen for encryption. This key is agreed between the buyer and seller during the contract. The composed message is encrypted using the shared key by the DES (Data Encryption Standard) algorithm. The message is scrambled in order to ensure additional security. This encrypted message is denoted as M_e

C. Image Moment Normalization

The source image is normalized based on its central moments. Moment normalization is much a useful technique as the moments of an image can be used to describe its contents with respect to the axes. Moments can be used to characterize images and to express properties that have analogy in statistics. Moment Normalization is done mainly to resist geometrical attacks [5] [6]. The steps of normalization are given below:

1. Compute the centroid of image ***I***
   $xbar = M_{10} / M_{00}$
   $ybar = M_{01} / M_{00}$
   where M_{ij} is defined as
   $M_{ij} = \sum\sum x^i * y^j * \boldsymbol{I(x,y)}$
2. Compute the central moments
   $\mu_{ij} = \sum\sum (x - xbar)^i * (y-ybar)^j * \boldsymbol{I(x,y)}$
3. Compute the covariance matrix based on the moments as CoV
   $$\begin{pmatrix} \mu_{20} & \mu_{11} \\ \mu_{11} & \mu_{02} \end{pmatrix}$$
4. Compute the eigen vectors of CoV
   $$\begin{pmatrix} e1x & e1y \\ -e1y & e1x \end{pmatrix}$$

   and the eigen values of CoV

   $$\lambda i = \tfrac{1}{2} * (\mu_{20} + \mu_{02}) \pm \sqrt{(4\mu^2_{11} + (\mu_{20} - \mu_{02})^2)}$$

5. Compute the orientation angle
   $\theta = \tfrac{1}{2} * \tan^{-1} (2\ \mu_{11} / (\mu_{20} - \mu_{02}))$
6. Compute the rotation matrix ***R*** as
   $$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$
7. Compute the scaling matrix ***S***
   $$\begin{pmatrix} (\lambda_1 \lambda_2)^{0.25} / \sqrt{\lambda_1} & 0 \\ 0 & (\lambda_1 \lambda_2)^{0.25} / \sqrt{\lambda_2} \end{pmatrix}$$
8. The translation matrix ***T*** is the eigen vector CoV
9. Construct the moment normalized image $\boldsymbol{I_m = R\ S\ T * I(x,y)}$

Thus the source image is moment normalized, so that it can withstand affine transformation attacks. Further details of image normalization using central moments are available in [1] [3].

D. Construction of Content Dependent Watermark

Wavelet transforms are perhaps a better method to analyze and understand the image [7]. Hence this scheme uses the wavelet domain to extract the watermark. The entire image is transformed using the Daubechies discrete wavelet transformation (DWT) up to level – 2. The coefficients in the level - 2 are considered for modulation to insert the watermark. The watermark construction algorithm is shown below:

1. The level - 2 of the wavelet-transformed image is divided into blocks of size 8x8.
2. The mean of each block is computed (B_m)
3. The mean of median filter of each block, (MB_m) based on the block mean is computed as
   $$MB_m = \sum_{k=i-B_m/2}^{k=i+B_m/2} I_b(x,y) / B_m$$
   where B_m is the local block mean.
4. The difference between block mean and the median filter mean of each block is computed as the content dependent watermark.
   $W_m = B_m - MB_m$
5. The encrypted message is set to be of same length as the number of coefficients in the level – 2 of the transformed image.
6. The watermark is computed as the difference between the value of the difference in means and the encrypted message.
   $W = W_m - M_e$
7. The watermark W is adjusted to the coefficients in the mid frequency components of the wavelet transformed image in level – 2 blocks denoted by I_{22} and I_{23}:
   $I_{22} = I_{22} + W$ (Low High Band)
   $I_{23} = I_{23} – W$ (High Low Band)
8. After the coefficient modulation is done for all the blocks, the image is reconstructed using the inverse wavelet transform.

Thus content dependent watermark is constructed and coefficients are modulated to perform watermark insertion.

E. Inverse Normalization of Watermarked Image

The modulated image is inverse moment normalized by computing the inverse of the rotation, scaling and translation matrices ***R, S*** and ***T.*** The watermarked image ***I**** is constructed and sent to the receiver.

$$I^* = R^{-1} * S^{-1} * T^{-1} * I$$

F. Parameters to be Considered for Watermarking

A set of parameters has been discussed for designing a watermarking system [4]. *Amount of embedded information* is an important parameter as it directly influences the watermark robustness. It is clear that the more the information to embed, the lower the watermark robustness. *Size and Nature of Image* plays a vital role on the watermark robustness. Although very small pictures have not much of commercial value, any watermarking scheme should be able to recover the watermark. *Secret Key* has no direct impact on the image fidelity, but plays an important role in the security of the system. The key space must be very large to make exhaustive search attacks impossible.

G. Watermark Detection

Watermark detection is a simple process. The received image is sent to the detection algorithm. The same steps as that of insertion are followed and the hidden watermark in extracted from the Level -2 coefficients. The watermark is constructed simultaneously. The extracted and constructed watermarks are compared. If they compare favorably, the image is said to be authentic else the image is declared to have been tampered. Comparing the watermarks on a bit-by-bit basis can easily identify the tampered locations.

H. Applications

This proposed scheme could be used in a wide range of applications wherever images are vital. Major applications are in validating identity cards such as debit and credit cards, voter identity cards, driving licenses and employee identity cards. Another major application is in authenticating financial instruments such as fixed deposit receipts and financial stock.

III. Performance Evaluation

The proposed scheme is a blind watermarking scheme and hence, the watermark extraction procedure can be done without using the original image. The effects of various types of attacks on the proposed scheme are analyzed.

A. Resistance to Geometric attacks

With moment normalization the proposed scheme has the ability to withstand geometrical attacks such as, removal of rows or columns as well as shifting rows or columns, changes in aspect ratio (as only one bit is inserted in each block). As the embedding procedure is based on the features of the block and moment normalization, this scheme is able to resist other geometric distortions including scaling, flipping and rotation.

B. Benchmarking and Performance Evaluation

This section deals with various benchmarking parameters [4] used to verify the robustness of the scheme. For fair benchmarking and performance evaluation, the visual degradation due to embedding is an important issue. Most distortion measures (quality metrics) used in visual information processing belongs to a group of *difference distortion measures*. Table I lists the commonly used measures. Let I denote the original image (Seller Image) of size $m \times n$ and I^* denote the watermarked image (Buyer Image) of same size.

TABLE I
COMMONLY USED PIXEL-BASED DISTORTION METRICS

1) Pixel Based Metrics	
Maximum Difference (MD)	$\max(I - I^*)$
Average Absolute Difference (AAD)	$1/mn * \sum \lvert (I - I^*) \rvert$
Norm Avg. Absolute Difference (NAD)	$\sum \lvert (I - I^*) \rvert / \sum \lvert I \rvert$
Mean Square Error (MSE)	$1/mn * \sum (I - I^*)^2$
Normalized MSE (MNSE)	$\sum (I - I^*)^2 / \sum I^2$
L^p Norm	$(1/mn * \sum (\lvert I - I^* \rvert)^p)^{1/p}$
Signal to Noise Ratio (SNR)	$\sum I^2 / \sum (I - I^*)^2$
Peak Signal to Noise Ratio	$mn * \max(I^2) / \sum (I - I^*)^2$
Image Fidelity	$1 - \sum (I - I^*)^2 / \sum I^2$
Correlation Distortion Metrics	
Normalized Cross Correlation	$\sum I \; I^* / \sum I^2$
Correlation Quality	$\sum I \; I^* / \sum I$

C. Acceptable Attacks

The proposed scheme is capable of resisting a set of attacks. These attacks may be either malicious or intentional. More details about these attacks are available in [4]. The types of attacks that the scheme is resilient to are: *JPEG Compression, Geometric Transformations* and *Image Enhancement Technique.*

IV. Math

This section discusses the experimental results of the proposed scheme. The algorithm has been implemented using Matlab 6.5. and the attacks on the images have been done using Adobe Photoshop 7.0. The algorithm has been tested on nearly 50 sample standard images.

A . Watermarking Parameters

Standard images Lena, Baboon and clown have been shown for the verification of this scheme. The watermarking parameters have been configured as below: *Amount of embedded information:* 128 bits of data. *Size and Nature of Cover Image:* All chosen images are gray scale of size 256 x 256. *Secret Key:* The key chosen for encryption is a long random integer.

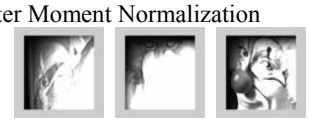
B. Watermarking Scheme

This section shows the images during the various stages of watermarking scheme. The results have been shown in a step-by-step manner.

1. Cover Images (Size: 256 x 256)

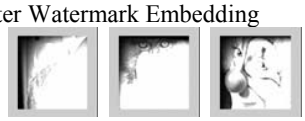
Lena Baboon Clown

2. Images after Moment Normalization



3. Images after Wavelet Transform

4. Images after Watermark Embedding



5. Images after Inverse DWT

6. Images after Inverse Moment Normalization (Watermarked Images)

Fig. 3 Resultant Images during various Phases of Watermark Insertion

C. Performance Evaluation Metrics

The various performance evaluation metrics have been listed and the values of these metrics are shown for the test images [4]. The results have been obtained by comparing the cover images with the watermarked images as in Table II, shows that all these metrics fall within a small range and hence the watermarked image and the original image do not have much of visual degradation. The various types of attacks discussed in section III C have been done on the same set of watermarked images and have been tabulated in Table III with the attacks on Lena. The results depict that the scheme can withstand these attacks if done either incidentally or maliciously.

V. Conclusion

The aim of this proposed algorithm is to construct a robust watermarking scheme that can withstand compression, removal and geometrical attacks. Discrete Wavelet Transforms have been used to extract features to serve as contents of the watermark. The concept of central moment normalization is to make the scheme withstand various geometric attacks. Benchmarking of this scheme has been done by estimating the pixel-based metrics and the correlation based metrics. This scheme is robust against content preserving modifications and easily identifies any content changing modifications. The major limitation of the proposed scheme is that it cannot resist copy attack and cropping attack. Thus this forms a future direction of work and the scheme can be extended towards guarding against protocol attacks, copy attack and cropping.

TABLE II
Performance Evaluation

Pixel Based Metrics	**Lena**	**Baboon**	*A. Clown*
MD	49.5	32.14	55.57
AAD	0.01	0.01	0.01
NAD	0.01	0.01	0.08
MSE	0.08	0.05	0.08
MNSE	4.91	5.00	1.71
L^2 Norm	0.28	0.24	0.29
SNR	2.03	1.99	5.82
PSNR	3.38	2.73	1.71
IF	0.99	0.99	0.99
MPSNR	26.80	27.81	26.64
NCC	0.99	0.99	0.99
CQ	122.36	132.51	86.26

TABLE III
Results after few Attacks on Lena

Lena Attacks	IF	MPSNR	CQ
JPEG	0.99	26.52	122.74
Horizontal Flip	0.99	27.68	124.51
Vertical Flip	0.99	27.44	124.59
Random Noise	0.99	26.57	121.61
Median Filter (3)	0.99	26.84	122.09
Gaussian Noise	0.99	26.56	123.64
Salt Pepper	0.99	26.79	121.87

References

[1] Tuang-Lam Le and Thi-Huango-Lan Nguyen, "Digital Image Watermarking with Geometric Distortion Correction using the Image Moment Theory", International Conference, RVIF, Hanoi, Feb 2004.

[2] J. J. K. O.' Ruanaidh and T. Pun, "Rotation Scale and Translation invariant spread spectrum digital watermarking" Signal Processing, 1998.
[3] M. Alghoniemy and A. H. Tewfik, "Geometric distortion through Image Normalization", Proceedings of International Conference on Multimedia Expo, 2000.
[4] M. Kutter, F A P Petitcolas, "A Fair Benchmark for Image Watermarking Systems", Electronic Imaging, The International Society for Optical Engineering, Jan 1999.
[5] M. Alghoniemy and A. H. Tewfik, "Image Watermarking by moment Invariants" Proceedings of IEEE international conference on Image Processing, Vancouver, 2000.
[6] P. Bas, J. M. Chassery and B. Macq, "Geometrically Invariant Watermarking using Feature Points", IEEE Trans. on Image Processing, Vol. 9, 2002.
[7] Latha Parameswaran, "Content Dependent Image Signature for Authentication Using Wavelets", Proceedings of NCIS, Karunya Deemed University,Coimbatore, Nov.2005.