A Hybrid Approach to Digital Image Watermarking Using Singular Value Decomposition and Spread Spectrum

Kunal Bhandari, Suman K. Mitra, and Ashish Jadhav

Dhirubhai Ambani Institute of Information and Communication Technology,
Gandhinagar, Gujarat, India, 382007
{kunal_bhandari, suman_mitra, ashish_jadhav}@da-iict.org

Abstract. This paper compares the most utilized spread spectrum technique with the newly evolved technique based on Singular Value Decomposition (SVD) for watermarking digital images. Both techniques are tested for a variety of attacks and the simulation results show that the watermarks generated by these techniques have complimentary robustness properties. A new hybrid technique, combining both paradigms, is proposed that is capable of surviving an extremely wide range of attacks. An image is first watermarked using spread spectrum and then a SVD based watermark is added to the watermarked image. The resulting double watermarked image is extremely robust to a wide range of distortions.

1 Introduction

Past few years have seen an explosive growth in digitization of multimedia (image, audio and video) content. The advancements in Internet technologies have largely increased the distribution of multimedia material. The possibility of infringement of digital media has also increased. The replication, manipulation and distribution of the digital multimedia content causes considerable financial loss to the media owners.

Digital watermarking [1] techniques offer a better solution as compared to encryption for the protection of such intellectual properties. Watermarking is a concept of embedding an unobtrusive mark into the data. This embedded information can later prove ownership, identify un-authorized copy, trace the marked data's dissemination through the network, or simply inform users about the rights-holder or the permitted user of the data. In sections 2, 3 and 4 we describe the basic spread spectrum approach, the SVD technique and the proposed hybrid scheme, respectively.

2 Watermarking Using Spread Spectrum [2]

Let N be the total number of pixels in an image, r_c be the chip-rate and $\{a_j\}$:($a_j \in \{-1,1\}$) be the sequence of information bits to be embedded into the image. Then the spread sequence,

$$\{b_i\}: b_i = a_j; \text{ where } \quad j.r_c \le i < (j+1).r_c \quad . \tag{1}$$

S.K. Pal et al. (Eds.): PReMI 2005, LNCS 3776, pp. 447 – 452, 2005.

The spread sequence $\{b_i\}$ is then modulated by a pseudo-noise sequence $\{p_i\}$, where $p_i \in \{-1,1\}$. The modulated signal scaled with α is arranged into a matrix with size equal to the image. The watermark, w_i, is added to the image pixel values, v_i, to give the watermarked image, v_i^*.

$$w_i = \alpha.b_i.p_i \qquad \text{and} \qquad v_i^* = v_i + w_i \ . \tag{2}$$

The watermark could be extracted by means of a correlation receiver. The original image is first subtracted from the watermarked image to remove components of the image itself. The second step is demodulation, which is the multiplication of the subtracted watermarked image with the same pseudo-noise signal $\{p_i\}$ that was used for embedding. This is followed by summation over a window of length equal to the chip rate, yielding the correlation sum S_j for the j^{th} information bit. Therefore

$$S_j = \sum_{i=j.r_c}^{(j+1)r_c-1} p_i.w_i = \sum_{i=j.r_c}^{(j+1)r_c-1} p_i^2.b_i.\alpha = a_j.r_c.\alpha \ . \tag{3}$$

Now, sign (S_j)=sign $(a_j.r_c.\alpha)$ = sign (a_j). This is because $r_c > 0$, $\alpha > 0$, $p_i^2 = 1$ and $a_j = \pm 1$. Thus the embedded bit can be retrieved without much loss. Therefore the embedded information bit is 1 if the correlation is positive and -1 if it is negative.

3 Watermarking Using Singular Value Decomposition [4] [5]

Singular value decomposition (SVD) is a linear algebra technique used to diagonalize matrices (image in this case) and it packs most of the signal energy into very few singular values (SVs). The SVs of an image remain un-changed even if the image is perturbed. This property is primarily used in image watermarking. Let the SVD of the host image X (M x N: M≥N) and the watermark W (P x Q: P≥Q) are as follows,

$$X=U\,S_x\,V^T \qquad \text{and} \qquad W=U_w\,S_w\,V_w^T \ . \tag{4}$$

Here S_x and S_w are diagonal matrices and represent the SVs of X and W, respectively and are represented by $S_x = [K_{x1}\ K_{x2}\ldots..K_{xN}]$ and $S_w = [K_{w1}\ K_{w2}\ldots..K_{wQ}]$. The watermark is embedded into the singular values of X according to the relationship

$$S_y = [K_{y1}\ K_{y2}\ \ldots\ K_{yN}] \qquad \text{where, } K_{yi} = K_{xi} + \gamma.K_{wi} \ . \tag{5}$$

Here γ is a scaling factor that determines the embedding strength and accounts for the perceptual quality of the watermarked image Y $(Y=U\,S_y\,V^T)$. The extraction process requires SVs of the host image and the watermark. The extraction process is as explained in (6). Here Y* is the possibly attacked watermarked image and W* is the recovered watermark.

$$Y^* = U^*\,S^*_y\,V^{*T},\ S^*_w=(S^*_y - S_x)/\gamma, \text{ and } W^*=U_w\,S^*_w\,V_w^T \ . \tag{6}$$

4 Proposed Scheme

The SVD watermark interferes with the original image and original image is needed at the receiver to extract the watermark. It increases the robustness against attacks of low pass nature like blurring and lossy compression [3] [4] [5]. It also provides good performance against rotation attack [3]. It is susceptible to histogram based attacks and addition of noise. The spread spectrum based noise like watermark is statistically orthogonal to the host image and is spread throughout the image [2]. It uses correlation sum to extract the watermark and is highly sensitive to resynchronization attacks [6]. It performs quite well for addition of noise and gamma correction.

The range of attacks, these two techniques survive or succumb, are complimentary. Thus if we combine these two techniques then we can achieve robustness against a very wide range of intentional and unintentional attacks. We propose a hybrid SVD-SS method designed such that the two watermarks interfere very little with each other. The host image is marked with a spread spectrum based watermark and then the resulting image is re-watermarked using the SVD approach. The proposed scheme enjoys the benefits of both the methods and at least one of the watermarks survives under various attacks. The proposed embedding method is shown in Fig.1. The recovery procedure is just a reverse mechanism of embedding.

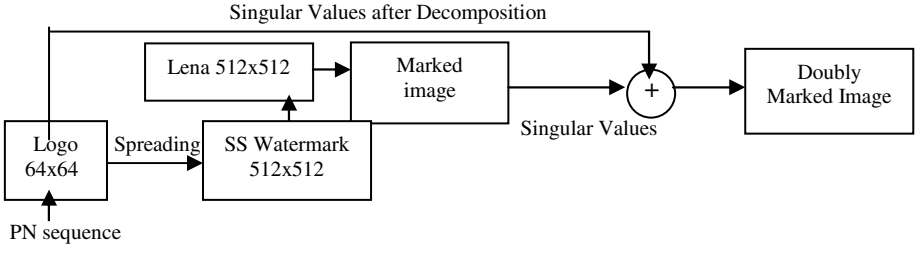

Fig. 1. Block diagram representing the embedding process of the proposed scheme

5 Experimental Results

The standard Lena 512 X 512 uncompressed image was used as the host and DA-IICT logo 64 X 64 as a binary watermark. The parameters r_c, α and γ for the embedding process are taken as 64, 5 and 50 respectively. The robustness of the algorithm is tested for 14 different attacks as illustrated in Fig.2. The JPEG compression, rotation, addition of Salt & pepper and Gaussian noise, intensity adjustment, gamma correction, histogram equalization, median filtering and dithering are applied from inbuilt functions of MATLAB. Attacks like Pixelate5 (Mosaic) and intentional pixel exchange are done in Photoshop. Print and scan (300dpi) is also considered as an attack.

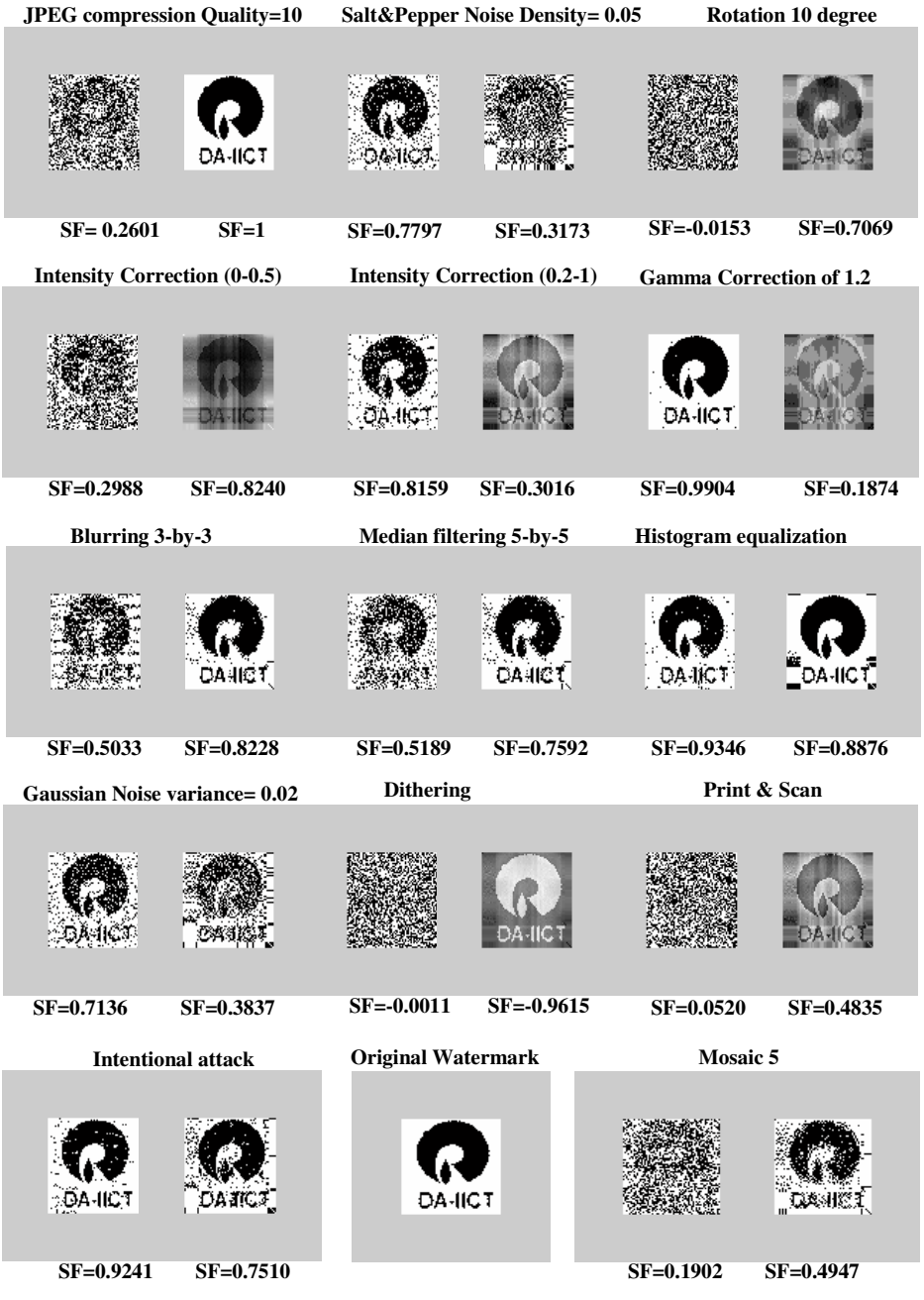

Fig. 2. Watermarks, with the similarity factors (SF), recovered after various attacks on the doubly marked image. The first logo shown, for each attack, is the one recovered by spread spectrum and the second by SVD extraction methods. The original logo is also shown.

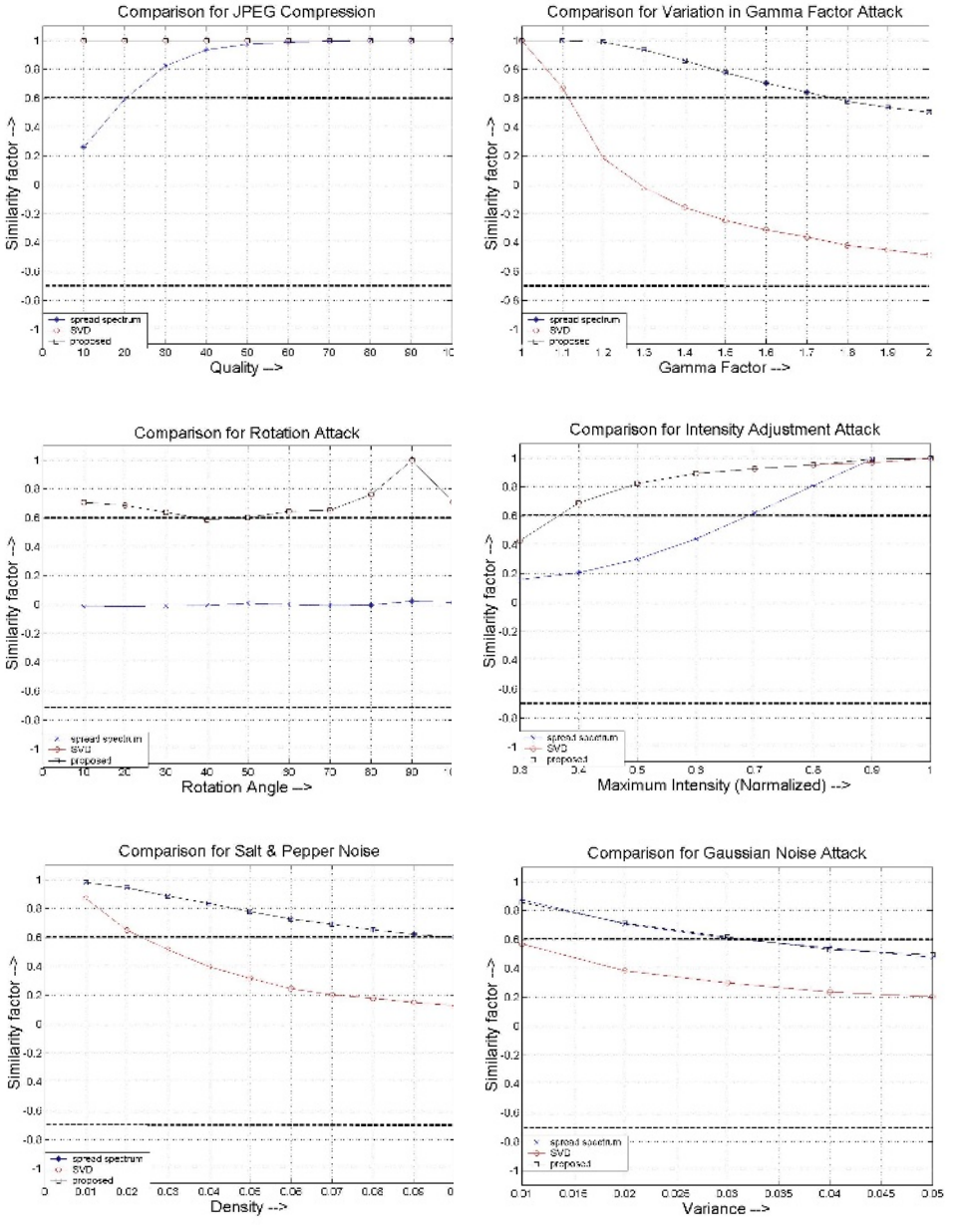

Fig. 3. Various plots showing comparison between SVD, Spread spectrum and the proposed hybrid scheme

The spread spectrum approach survives addition of noise, intensity adjustment k to 1 (k>0) and gamma correction while the SVD based approach outperforms spread spectrum in rotation, cropping, JPEG compression for quality below 30, intensity adjustment 0 to k (k<1) and filtering attacks. The extracted watermark W* is

correlated with the original watermark W to quantitatively measure the similarity. It ranges between -1 to 1. More is the similarity factor better is the retrieval of the watermark. Fig.3 shows plots of similarity factors for various attacks. It is evident from Fig.3 that the performance of the proposed method is better than a non-hybrid scheme employing either of the techniques. It has been observed that under some attacks the visual quality of the extracted watermark is poor even if the similarity factor is high. By applying proper scaling, the visual quality of such watermarks can be enhanced. The simulation results validate our assertion that the proposed algorithm is resilient to a very broad category of intentional and unintentional attacks.

6 Conclusion

This paper presents a novel SVD-SS hybrid watermarking technique that embeds two watermarks, one by spread spectrum and the other by SVD approach. The two techniques of embedding watermarks separately are found to be complimentary to each other as far as robustness against various attacks is concerned. The proposed scheme being a union of both the schemes, survives the union of the attacks survived by each scheme independently. The scheme is designed such that there is negligible degradation of the image on addition of the second mark.

References

1. I. Cox, M. Miller and J. Bloom, “Digital Watermarking,” Morgan Kauffman Publisher, 2001.
2. M. George, J. Y. Chouinard and N. Georganas, “Digital Watermarking of Images and Video using Direct Sequence Spread Spectrum Techniques,” IEEE Canadian Conference on Electrical and Computer Engineering, vol. 1, 9-12 May 1999, pp. 116 – 121.
3. R. Liu and T. Tan, “A SVD-Based Watermarking Scheme for Protecting Rightful Ownership,” *IEEE Transactions on Multimedia*, 4(1), March 2002, pp.121-128.
4. Chandra D.V.S, “Digital Image Watermarking using SVD”. Circuits and Systems, MWSCAS-2002., vol. 3 , 4-7 Aug. 2002, pp.III-264 - III-267.
5. V.I. Gorodetski, L.J. popyack, V. Samoilov, and V.A. Skormin, “SVD-Based Approach to Transparent Embedding Data into Digital Images” proc. Int. Workshop on Mathematical Methods, Models and Architecture for Computer Network Security, LNCS, Vol. 2052, pp. 263-274, Springer Verlag, 2001.
6. F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," in Security and Watermarking of Multimedia Contents, Proc. SPIE 3657, Jan. 1999, pp.147-158.