International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-8 March-2013

An effective algorithm for Image security based on Compression and Decomposition method

Seetaiah Kilaru[1], Yojana Kanukuntla[2] and K B S Chary[2]
Research Scholar, University of Birmingham, England[1]
Electronics & Communication Engineering Department, Swarna Bharathi Institute of Science & Technology[2]

Abstract

Security is the main concern in any field. With the frequent attacks, it is a big challenge for the users to protect the digital images which are transmitting over internet. Singular Value Decomposition (SVD) [7] provides a solution up to a greater extent. This paper mainly concentrates on the invisible watermarking. By using the Wavelets, invisible watermark embed into the original watermark. The main focus concentrated on the wireless communications; hence it is important to consider some factors into consideration, they are size of an image and requirements of bandwidth. Keeping in view of all these parameters, compression and transmission should be done. The proposed algorithm uses the SVD method along with compression. The proposed algorithm is robust against all common attacks which exist in image processing field. Tests have been done and results are satisfactory in terms of imperceptibility and security.

Keywords

Singular Value Decomposition, Compression, Image histogram, Correlation coefficient, Structural Similarity Index Measure (SSIM), Similarity index

1. Introduction

All The application of multimedia over internet is playing major role in current scenario. Web applications are also designing with the features of fast computation and convenient. The sending of document contains secret or important images for the intended user without participation of unknown third party is always a tough challenge [2]. The ownership and Authentication are challenging tasks for the users to protect their information. Current existing Digital Watermarking Techniques plays a vital role to protect the data and to define the right ownership. The increased hacking and other web technologies are trying to modify the watermarking process [5]. Then it is a new challenge for the researchers to implement effective watermarking technique which provides security. A digital watermark [3] is a unnoticeable cover work which hides the owner information. There are various watermarking techniques available in the market. Broadly, there are two types of watermarking. They are visible and invisible watermarks. The watermarking technique [3, 4] is said to be robust only when it resists all possible attacks. In this paper, Singular Value Decomposition (SVD) method help taken to define and design the perfect watermarking process which increases the security. The combination of image features with SVD and digital watermarking algorithm were implemented by using the wavelet phenomenon [2,6,8]. This process concentrates on content watermarking rather than pixel watermarking.

2. Background

The property of human perception is giving us a chance to accept small distortion. These small distortions are not possible to determine with our eye. The theory of HVS model [11] also suggested same principle. In linear algebra, SVD plays a significant role and it is used by renowned mathematicians. It can be performed on any matrix of order (m.n). For example, a matrix M has m rows and n columns with the rank r such that r ≤ *n* ≤ *m*. Then the matrix can be represented as USV^T [1].

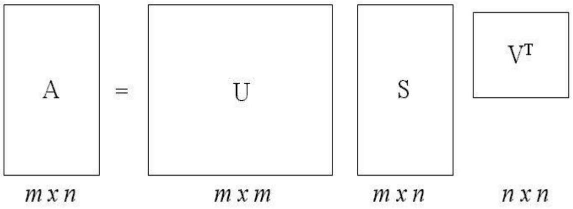

Figure 1: Matrix Representation

Where Matrix *U* is an *m* × *m* and V is the *n* × *n* orthogonal *matrices*.

U= [u_1,u_2,u_3,....u_r,u_{r+1},...u_m]

$$\mathbf{u}_i^T \mathbf{u}_j = \delta_{ij} = \begin{cases} 1,,\, i = j \\ 0,,\, i \neq j \end{cases}$$

$$V = [\mathrm{v}_1, \mathrm{v}_2, \ldots \mathrm{v}_r, \mathrm{v}_{r+1}, \ldots, \mathrm{v}_n]$$

$$\mathrm{v}_i^T \mathrm{v}_j = \delta_{ij} = \begin{cases} 1,,\, i = j \\ 0,,\, i \neq j \end{cases}$$

Let us consider, S is the singular value diagonal matrix, such that

$$S = \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \sigma_{r+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \sigma_n \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

3. Quality Analysis

It is common practice to analyse the performance of the system to know how much effective when compared to the existing system. There are various parameters are available to check the robustness and peak SNR values. The image analysis also explains about the efficiency of the system against attacks. The following are the some of the parameters to analyse quality of an image.

Normalised Hamming Distance (NHD):

This is the measurement of similarity which measures the ration of similarity index between original tested image and output image. The definition of the NHD [7] in mathematical form can be written as

$$\mathrm{NHD}(\mathrm{w}, \mathrm{w}') = \frac{1}{\mathrm{N_w}} \sum_{i=1}^{\mathrm{N_w}} \mathrm{w(i)} \oplus \mathrm{w'(i)}$$

Here, w represents test image watermarked image and w' represents the extracted watermarked image. N_w is the length of watermark. The defined ranges for the equation are 0-1.

Peak Signal to Noise Ratio (PSNR):

It is one of the absolute measurements of quality between the tested watermarked image and distorted watermarked image [7]. The value represented in a single number with the unit of decibels. That value shows matching of similarity.

Let us consider the tested image w(i.j) with the M rows and N columns and distorted image is W'(i,j). The calculation of the error depends on the luminance calculation and also pixel position arrangement. The luminance of any pixel varies in between 0 and 255. To measure PSNR of an image it is suggested to measure Mean Square Error (MSE). The MSE is defined as

$$\mathbf{MSE} = \frac{\sum\sum[\ \mathbf{w(i,j) - w'(i,j)]2}}{\mathbf{MN}}$$

The PSNR is defined as

$$\mathbf{PSNR = 10\ log_{10}\ (MAXi^2\ /\ MSE)}$$

Index Measure Analysis:

Let us consider the tested image w(i.j) with the M rows and N columns and distorted image is W'(i,j). Then the similarity index measurement can be defined [7] as

$$\mathbf{SIM = \sum\sum w(i,j) * w'(i,j)\ /\ \sum\sum[w'(i,j)]2}$$

4. Watermark embedding scheme

1. The Define the image which is to protect and set the image for dividing into number of blocks.
2. It is suitable to divide the image into block ratio of 8 × 8. [4]
3. For every block apply singular value decomposition method and obtain the SVD.
4. Select the watermark which is to embed and read it.
5. Before embedding, try to perform addition of secret key (Recommended)
6. According to the pattern (bit pattern) of watermark, change the diagonal vector S of each block.
7. By remainder of the diagonal vector S (1,1) divided by the set value the image quality 'Q' factor.
8. For all changed vectors, calculate inverse SVD by using the concept of modulation by watermark.
9. Now, combine all blocks to construct final watermarked image.
10. Compress the image until it is suitable for the mobile transmission. [3,5]

The following figure shows the process of embedding watermark for the image Lena

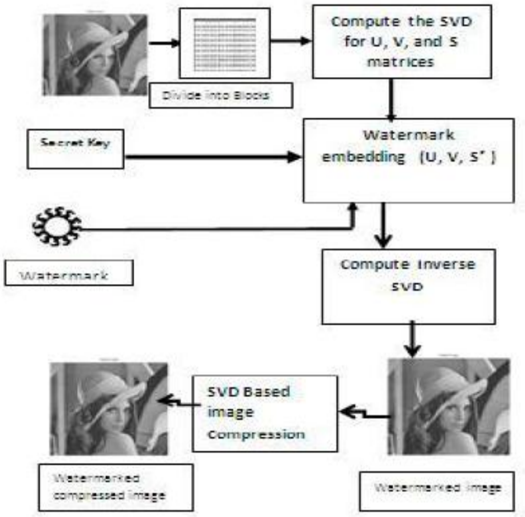
Divide into Blocks
Compute the SVD for U, V, and S matrices
Secret Key
Watermark embedding (U, V, S')
Watermark
Compute inverse SVD
SVD Based image Compression
Watermarked compressed image
Watermarked image

Figure 2: SVD based image watermarking and compression scheme

5. Experimental results

For experimental purpose, different images are tested. By using SVD method, embedding process possible in smooth way. Lena is taking as a reference image to do the watermark procedure. The good algorithm is always robust against attacks. Attacks are common in these type of proceedings especially signal processing and geometric attacks.

Used versions: Windows XP, 1 GB RAM, 2.3GHz CPU and for program development MATLAB was used.

Histogram analysis:

By considering intensity of pixel as a reference, we obtain Histogram. The following figure (a) shows test image and (b) shows the logo of the watermark. Figure (c) represents final watermarked image. This watermarked image is also compressed by compression method. Figure (d) shows histogram of (c). From all these results, we can conclude that, our human eye is not able to find out the difference between images.

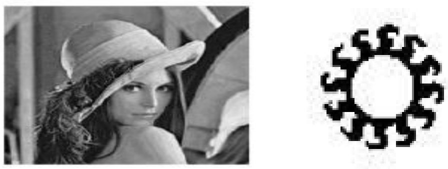

Figure 3: Original test image and watermak logo

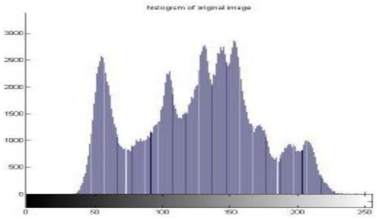

Figure 4: Histogram of original image

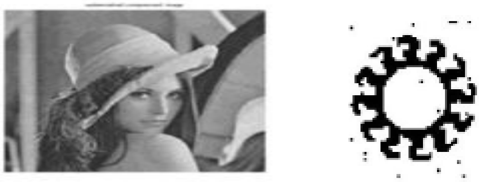

Figure 5: compressed and watermarked image; recovered logo

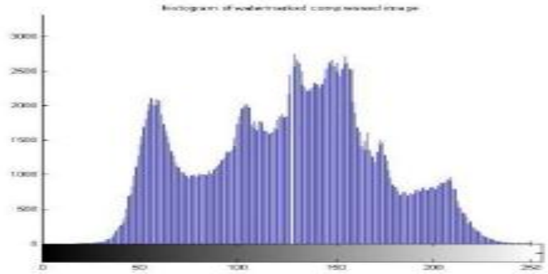

Figure 6: compressed and watermarked Histogram

Correlation coefficient analysis:

Correlation coefficient analysis is carried for adjacent pixel of the encrypted images of different test images between horizontally, vertically and diagonally adjacent pixels. From the experiment, it is clear that scrambling phenomenon was reversed for all the pixel f the adjacent pixels.

The correlated function is defined as

$$\mathrm{cov}(x,y) = 1/n \sum [\, E(x\_i - E(x))(y\_i - E(y))]$$

$$r\_xy = \mathrm{cov}(x, y) / (\mathrm{sqrt}(D(x) * D(y)))$$

Where r represents correlation coefficient between all possible cases like diagonal, vertical and etc.

$$D(x) = 1/n \sum \mathrm{square}\, [(x\_i - E(x))]$$

$$E(x) = 1/n \sum (x\_i)$$

For the correlation coefficient of horizontal pixel is 0.9898, the horizontally spaced adjacent image characteristics is as follows:

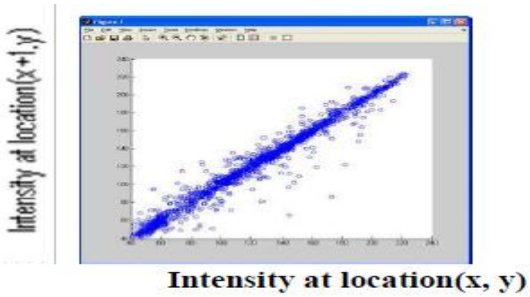

Figure 7: plot of horizontally spaced test image for coefficient = 0.9898

For the correlation coefficient of horizontal pixel is 0.9785, the horizontally spaced adjacent image characteristics is as follows:

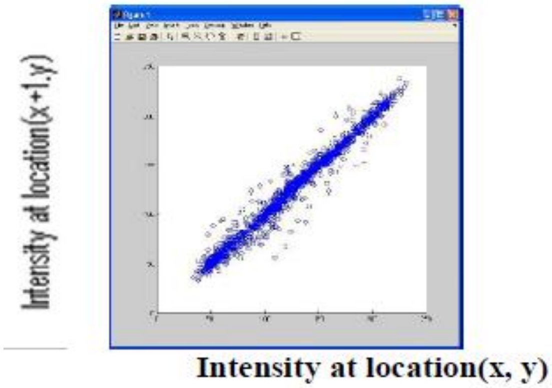

Figure 8: plot of horizontally spaced test image for coefficient = 0.9785

Index measure analysis:
The basic index parameter in this analysis is similarity. Hence, this method is also called as Structural Similarity Index Analysis (SSIA). The inventor of this process was Wang. The main parameter in this scheme was correlation of output with the Human Visual System (HVS). The main parameters of this method are luminance (l), contrast (c) and comparision of structures (s). Hence it can be defined as a function of all these three elements.

$$\mathrm{SSIM}\ (f\ g) = l\ (f\ g)\ c\ (f\ g)\ s\ (f\ g)$$

The range of SSIA lies between 0 and 1.
SSIA = 0 when there is no correlation and
SSIA = 1 when there is a maximum correlation.

SSIA values for the original and reference test image.

Table 1: SSIM values of original vs reference test images

Name of Reference Image	Original image SSIM	Watermarked and compressed SSIM
Clown	1	0.8765
Crowd	1	0.8732
Lena	1	0.8896

Peak Signal to Noise Ratio (PSNR):
it is also one of the best method in image processing analysis. High PSNR result analyze about efficiency of designed algorithm and complexity of system. The following table shows the output results of different images i.e. original and test images.

Table 2: PSNR comparision

Name of Reference image	Test image PSNR	Test and watermarked image PSNR
Clown	39.43	32.52
Couple	39.57	30.69
Lena	39.12	31.46

Attacks on images:
In wireless process of transmission there are variety of chances to undergo noise attack on images. The designed algorithm is called as robust only when it resists all attacks of an image. The added noise has different type of forms viz.. Pseudo Random Noise generation or poisson distributed noise generation. It depends on the environment from where we are proceeding. The following statistics gives a clear idea about the process of recovering of an image from several attacks.

Guassian noise attack:
If the guassioan noise parameters are μ = 0.01 and Ϭ = 0.001 then the watermarked image and logo look like as

Figure 9: for μ = 0.01 and Ϭ = 0.001, watermarked image and watermark logo under Guassian noise

The following table shows the comparision between original/test watermarked image and the image recovered from the guassian noise.

Table 3:PSNR values of original vs watermarked and original Vs Watermarked and compressed images

Name of Reference Image	Correlation coeficient	Hamming distance	Index measure (structural similarity)
Clown	0.4978	0.1432	0.8156
Couple	0.6546	0.0984	0.8967
Lena	0.7102	0.1058	0.9043

Frequency attack:
In median filtering process, every pixel in selected mask should be replaced by the value which is median or average of all pixels. the selected mask size depends on the application and requirement of the system. The term median is always less sensitive than mean and hence it is easy to remove the outliers without any distrubance to the sharpness to the image. In this analysis MIDFILT2 function is used.

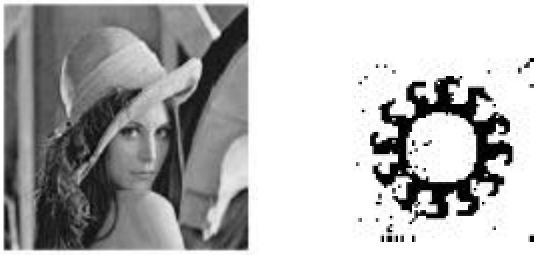

Figure 10: attacked image and extracyed logo from the watermarked image

The following table shows the analysis of original test image and recovered image (median filter)

Table 4: Image analysis between the original watermark and the watermark recovered from the attacked watermark image with Gaussian noise

Name of Test image	Correlation value	Hammin distance	Index measure
Clown	0.7834	0.0643	0.9314
Couple	0.6984	0.1206	0.9123
Lena	0.9365	0.0198	0.9786

6. Conclusion

The paper describes about the robust watermarking technique based on SVD. Based on the quality of different parameters, the algorithm was designed. Experiments results were satisfactory in PSNR, Similarity index and performance against attacks. Finally, we conclude that, this watermark technique is useful in real time applications and in transmitting applications against all common attacks.

References

[1] Chu, W. C., DCT-Bbased image watermarking using subsampling, IEEE Transactions on Multimedia, vol.5, no.1, pp.34-38, 2003.

[2] Tapas Bandyopadhyay, B. Bandyopadhyay, B N Chatterji, Image Security Enhancement Through Watermarking and Cryptographic Measures, National conference : INDIACOM-2009 , New Delhi ,February 2009.

[3] Hou, Z., Adaptive singular value decomposition in wavelet domain for image denoising, Pattern Recognition, vol.36, no.8, pp.1747-1763, 2003.

[4] Cox, I. J., J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, vol.6, no.12, pp.1673-1687, 1997.

[5] Eleni Drinea, Petros Drineas and Patrick Huggins A Randomized Singular Value Decomposition Algorithm for Image Processing Applications.

[6] Habibollah Danyali, Morteza Makhloghi and Fardin Akhlagian Tab “Robust blind DWT based digital image watermarking using singular value decomposition”.

[7] Alain Horé and Djemel Ziou “Image quality metrics: PSNR vs. SSIM” 2010 International Conference on Pattern Recognition.

[8] Rowayda A. Sadek, “SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges”.

[9] SeungJae Lee Dalwon Jang and Chang D. Yoo “An SVD-Based Watermarking Method for Image Content Authentication with Improved Security” Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on 2005 pages: 525-528.

[10] B.Chandra Mohan and S. Srinivas Kumar “A Robust Image Watermarking Scheme using Singular Value Decomposition “journal of multimedia, vol. 3, no. 1, may 2008.

[11] Peter FORIS and Dušan LEVICKÝ, “Implementations of HVS Models in Digital Image Watermarking “ , Radioengineering, vol. 16, no. 1, april 2007.

Yojana Kanukuntla received her Master of Technology from Kakatiya University, Andhra Pradesh. Her major researches areas include Signal, Image and Video processing. She guided more than 18 M.Tech projects and 38 B.tech Projects. Currently, she is working as a Associate professor in the department of Electronics & Communication Engineering Department, SBIT, KHAMMAM, AP.

Seetaiah kilaru received his Masters degree in Telecommunication Engineering from Staffordshire University United Kingdom. He worked as a project member in CISCO Laboratories as a junior research fellow in UK. Currently, he is working as Assistant Professor in the department of Electronics & Communication Engineering Department, SBIT, KHAMMAM, AP

Dr K B Srinivasa Chary, received hid Ph.D from Osmania University in 1990 and MSc from Osmania University in 1965. He joined as Junior Scientist in DRDo in 1967 and also worked as a senior scientist (Grade-I) till 2004. His areas of interest include electronic warfare systems and communication systems. Currently, he is working as a Professor in the department of Electronics & Communication Engineering Department, SBIT, Khammam, AP.