A ROBUST IMAGE WATERMARKING SCHEME USING SINGULAR VALUE DECOMPOSITION FOR COPYRIGHT PROTECTION

T.Geetamma[1], J Beatrice Seventline[2]

[1]Asst. Professor, Dept. of ECE,GMR Institute Of Technology, Rajam,(India)

[2]Assoc.Professor, Dept. of ECE,GITAM Univeristy, Vishakapatanm,(India)

ABSTRACT

In the current globalized world, the right of ownership is at stake. This is arises due to the easy exchange of data through various channels of communications and lack of authentication. The problem of piracy can be curbed to a large extent by using a technique called Digital Watermarking. The requirements of a formidable watermark are robustness, invisibility, undetectability, security. The main aim of this paper is to increase robustness by implementing the digital watermarking using Singular Value Decomposition(SVD). In this the host image is partitioned into four sub images. Watermark image is embedded in the two of these sub images, in both D and U components of SVD of two sub images. Watermark image is embedded in the D component using Dither Quantization. A copy of the watermark is embedded in the columns of U matrix using comparison of the coefficients of U matrix with respect to the watermark image. For extracting the watermark first the watermarked image is divided into four sub images and the proposed algorithm is applied.

Keywords - Copyright, Digital Watermarking, Steganography , Authentication

I. INTRODUCTION

In the past several years there has been an explosive growth in digital imaging technology and applications. With this growth Digital images and video are now widely distributed on the Internet and via CD-ROM. Digital data, such as digital audio, images, and video, can be stored, copied, and distributed quickly, easily, and without any loss of fidelity. The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service for both wired and wireless networks have made it possible to create, replicate, transmit, and distribute digital content in an effortless way. This frequent use of the Internet has created a need for security. One problem with a digital image is that an unlimited number of copies of an "original" can be easily distributed and/or forged. This presents problems if the image is copyrighted. The protection and enforcement of intellectual property rights has become an important issue in the "digital world." As a consequence, to prevent information which belongs to rightful owners from being intentionally or unwittingly used by others, information protection is indispensable.

Many approaches are available for protecting digital images and video; traditional methods include encryption, authentication, and time stamping. In this project we present algorithms for image authentication and forgery prevention known as **Digital Watermarking[1][2]**. A digital watermark is a signal that is embedded in a digital image or video sequence that allows one to establish ownership, identify a buyer, or provide some additional information about the digital content.

One approach for copyright protection is to introduce an invisible signal, known as a digital watermark, into an image or video sequence. Digital watermarking of multimedia content has become a very active research area over the last several years. In recent years, the research community has seen much activity in the area of digital watermarking as an additional tool in protecting digital content. New companies dedicated to watermarking technology are emerging and products like Digimarc's Media Bridge are appearing.

Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in its protected form, the watermark remains in the content in its original form and does not prevent a user from listening to, viewing, examining, or manipulating the content. Also, unlike the idea of steganography, where the method of hiding the message may be secret and the message itself is secret, in watermarking, typically the watermark embedding process is known and the message (except for the use of a secret key) does not have to be secret. In steganography, usually the message itself is of value and must be protected through clever hiding techniques and the "vessel" for hiding the message is not of value. In watermarking, the effective coupling of message to the "vessel," which is the digital content, is of value and the protection of the content is crucial.

Watermarking is the direct embedding of additional information into the original content or host signal. Ideally, there should be no perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host signal. In some instances, the amount of information that can be hidden and detected reliably is important. It is easy to see that the requirements of imperceptibility, robustness, and capacity conflict with each other. For instance, a straightforward way to provide an imperceptible watermark is to embed the watermark signal into the perceptually insignificant portion of the host data. However, this makes the watermark vulnerable to attack because it is fairly easy to remove or alter the watermark without affecting the host signal.

To provide a robust watermark, a good strategy is to embed the watermark signal into the significant portion of the host signal. This portion of the host data is highly sensitive to alterations, however, and may produce very audible or visible distortions in the host data. Applications for digital watermarking include copyright protection, fingerprinting, authentication, copy control, tamper detection, and data hiding applications such as broadcast monitoring. Watermarking algorithms have been proposed for audio, still images, video, graphics, and text.

Digital image watermarking has received increasing attention in recent times due to rapid growth in the internet traffic. It is gaining popularity due to its significance in content authentication and copyright protection for digital multimedia data. Digital image watermarking techniques can be categorized into one of the two domains, viz., spatial and transform, according to the embedding domain of the host image. The simplest technique in the spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels. The data hiding capacity in these methods is high. However, these methods are hardly robust. Watermarking in transform domain is more secure and robust to various attacks. The basic philosophy in majority of the transform domain watermarking schemes is to modify transform coefficients based on the bits in the watermark image .In 2002 Sun et al proposed SVD based watermarking scheme, wherein the D component with a diagonal matrix is explored for embedding. The basic mechanism used was the quantization of the largest component with a fixed constant integer, called Quantization coefficient. A trade off can be achieved between transparency and robustness by varying the quantization coefficient. Later in 2005, Chang et al. [13] proposed a watermarking scheme based on the SVD domain. U matrix of SVD is used for the watermark embedding. The absolute difference between the two rows of U matrix is used for the watermark embedding. They explored the positive relationships between the rows of U and V matrices that are preserved after JPEG compression also. Chung [15] et al., proposed two notes on the SVD based watermarking algorithm. As per the proposal from Chung et al. if the watermark is embedded in the watermark embedding is in U and V^T matrices. Magnitudes of U and V matrix elements are very small and so, even a small modification in either U or V components alters the watermark retrieval. Many of the algorithms proposed above suffer from either with the poor robustness or non-blind in nature.

In this work, a watermarking scheme is proposed which is robust, reasonably good capacity (32x32 logo is embedded in 512x51e. image) and blind in nature. The proposed method uses SVD domain and Dither quantization for embedding the watermark in both D and U [13]. Magnitudes of D matrix coefficients are very high compared to both U and V. In the proposed method, the largest singular values of the host image (D matrix coefficients) and coefficients of the U matrix are modified to embed the watermark data such as logo. The host image is partitioned into four sub images. Instead of using the entire host image for watermark embedding, only two sub images of size 256x256 are used. This is to ensure that the visual quality of the watermarked image is not degraded. With the two sub images for watermark embedding, a reasonably good quality image with a Peak Signal to Noise Ratio of more than 40dB can be obtained.

The rest of this paper is organized as follows: section 2 will describe the Singular Value Decomposition. Section 3 will describe about Dither Quantitization, section 4 will describe about Proposed Method, section 5 will give implementation results and section 6 will give conclusions.

II. SINGULAR VALUE DECOMPOSITION (SVD)

Singular Value Decomposition (SVD) is a mathematical tool used to analyze matrices[9][10]. SVD is a widely used technique to decompose a matrix into several component matrices, exposing many of the useful and interesting properties of the original matrix. The decomposition of a matrix is often called a 'factorization'. Ideally, the matrix is decomposed into a set of factors (often orthogonal or independent) that are optimal based on some criterion. For example, a criterion might be the reconstruction of the decomposed matrix. The SVD, in general, represents an expansion of the original data in a coordinate system where the covariance matrix is diagonal. The eigen matrix in the singular value decomposition is explored for data embedding.

Any real mxn matrix A can be decomposed uniquely as

$$A = UDV^{T.}$$

Here U and V are orthogonal, and D is a square diagonal. That is $UU^T = I_{rank\ (A)}$, and $VV^T = I_{rank\ (A)}$, where U is rank (A) x m, V is rank (A) x n. D is rank (A) x rank (A) diagonal matrix given by,

$D = \text{diag}\ (\sigma_1, \sigma_2 \ldots \sigma_{rank\ (A)})$ ordered so that $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_{rank\ (A)} > 0$, are the singular values of A, or the square roots of the eigen values of AA^T and A^TA. Each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer.

If U = $(u_1, u_2, \ldots, u_n)$ and V = $(v_1, v_2, \ldots, v_n)$, then,

$$A = \sum_{i=1}^{r} \sigma \; u_i v_i^T. \text{ (where r is the rank of matrix A).}$$

SVD can also be used to determine the rank for the rank-deficient matrices. Ideally, a rank-deficient matrix may be decomposed into a smaller number of factors than the original matrix and still preserve all of the information in the matrix.

An example:

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 3 & 2 \\ 1 & 2 & 1 \end{bmatrix}, \text{ then } AA^T = A^TA = \begin{bmatrix} 6 & 10 & 6 \\ 10 & 17 & 10 \\ 6 & 10 & 6 \end{bmatrix}$$

The eigen values of AA^T, A^TA, are:

$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} 28.60 \\ 0.14 \\ 0 \end{bmatrix}$$

$$u_1 = v_1 = \begin{bmatrix} 0.454 \\ 0.766 \\ 0.454 \end{bmatrix}, u_2 = v_2 = \begin{bmatrix} 0.542 \\ -0.643 \\ 0.542 \end{bmatrix}, u_3 = v_3 = \begin{bmatrix} -0.707 \\ 0 \\ -0.707 \end{bmatrix}$$

The expansion of A is

$$A = \sum_{i=1}^{2} \sigma \; u_i v_i^T. \text{ (Since, here rank = 2)}$$

There are many approaches to SVD watermarking. One of them is to apply SVD to the whole image and modify all the singular values, i.e., add the watermark to the all the singular values. Embedding a watermark in the SVD domain results in very little perceptual difference and the largest of singular values changes very little for most common attacks. Other techniques of SVD watermarking include performing SVD in the frequency domain, that is performing the SVD on the DCT coefficients or the DWT coefficients of the image and then adding the watermark to the singular values. The addition of the watermark to the SVD coefficients in the DCT domain may be done in different ways.

The results of SVD watermarking have been very encouraging because of the high capacity of embedding watermark information in the singular values and the minimal change in the quality of the final watermarked image. One limitation of this scheme is the requirement of the original image as well as the original watermark/secret keys in order to extract the watermark from the watermarked image, for it is a non-blind watermarking scheme. Two of the important applications of SVD watermarking are to disable unauthorized access to content and copyright protection. Singular represent the algebraic properties of an image. Singular values possess the algebraic and geometric invariance to some extent. The properties of the singular value are reviewed as follows

1. Theorem of (SDV):-

If A E R^{mxn} , then there exist orthogonal matrices

$U=[u_1, u_2, u_3, \ldots\ldots, u_m]$ E R^{mxn} and $V=[v_1,\ldots\ldots v_n]$ E R^{mxn}

Such that $U^T AV = \text{diag}(\sigma 1\ldots.\sigma p)$.

Where, p=min (m,n), $\sigma 1 \geq \sigma 2 \geq \sigma 3 \geq \ldots\ldots \sigma p \geq 0$. σ i , i=1,2,…..p are the singular values of A . The singular values are the square roots of the eigen values $\lambda_{i\ of}$ AA^H or A^HA, i.e, $\sigma i = \sqrt{\lambda i}$.

2. Theorem of stability of SV:-

The stability of singular value indicates that , when there is little disturbance with A , the variation of its similar value is not greater than 2-norm of disturbance . 2-norm is equal to the largest singular value of the matrix.

3. Theorem of the scaling property:-

If the singular values of A^{mxn} are σ1…..σ k , the singular values of $\alpha * A^{mxn}$ are $\sigma 1^* \ldots.\sigma k^*$, then ∣ α ∣(σ1…..σ k)=($\sigma 1^* \ldots.\sigma k^*$).

4. Theorem of the rotation invariant property:-

If *P* is a unitary and rotating matrix, the singular values of *PA (rotated matrix)* are the same as those of *A*.

5. Theorem of the translation invariance property:-.

The original image *A* and its rows or columns interchanged image have the same singular values.

6. Theorem of the transposition invariance property:-

If $AA^Tu = \lambda^2 u$

Then , $A^TAv= \lambda^2 v$,

So that A and A^T have same singular values.

The above mentioned (stability of SV, scaling invariance of SV, rotational invariance of SV, translation and transposition invariance of SV) properties of SVD are very much desirable in image watermarking. When the watermarked image undergoes attacks like rotation, scaling and noise addition, the watermark can be retrieved effectively from the attacked watermarked image due to the above said properties.

III. DITHER QUANTIZATION

In an ideal watermarking scheme, one signal (a digital watermark) is embedded within another signal (host image) signal to form a third signal (watermarked image) signal. The embedding should be done in such a way that minimizes the distortion between the host signal and watermarked signal and maximizes the information embedding rate and robustness of the embedding. All the three requirements are usually conflicting, and hence embedding process must be designed to efficiently trade-off these requirements. In the Dither quantization based watermarking schemes, the embedded information modulates a dither signal and the host signal is quantized with an associated dithered quantizer. Dither quantization based schemes have considerable performance advantages over conventional spread spectrum based schemes. The conventional spread sprectrum embedding function combines the host image and the watermark image in a linear way, and hence the watermark image can be extracted with ease. In contrast, dither quantization based schemes effectively hide the exact value of the host signal.

In the proposed watermarking scheme, a binary watermark is embedded in the gray scale host image. A binary watermark image consists of '1's or '0's. Dither quantizers are quantizer ensembles. Each quantization cell in the ensemble is constructed from a basic quantizer. The basic quantizer is shifted to get the reconstruction point. The shift depends on the watermark bit. The basic quantizer is a uniform scalar quantizer with a fixed step size *T*. A quantizer in the ensemble consists of two quantizers shifted by *T/2* with respect to each other. The largest component of *D* matrix of an 8x8 block is quantized using either quantizer 1 or quantizer 2 that depends on watermark bit to be embedded. The quantized value is the center of the quantizer.

IV. PROPOSED METHOD

In the proposed method, the D matrix and U matrix are explored for embedding the watermark. The D component matrix contains the largest coefficients. These coefficients are modified in such a way that the watermark image quality is not degraded. The modification of the coefficients is based on the dither quantization. After the modification of singular values, inverse SVD is applied and the watermarked image is obtained. The watermark embedding algorithm is presented in the following steps:

4.1 Host image partition:

1. The host image f(i,j) of size N*N is partitioned into four sub images as shown in figure.

2. Four sub images $f_{tl}(p,q)$ (top left), $f_{tr}(p,q)$ (top right), $f_{bl}(p,q)$ (bottom left), $f_{br}(p,q)$ (bottom right) of the host image are defined as:

$f_{tl}(p,q)=f(i.j)$ $\quad 1 \leq i \leq N/2,$

$1 \leq j \leq N/2$

$f_{tr}(p,q)=f(i,j)$ $\quad 1 \leq i \leq N/2,$

$N/2+1 \leq j \leq N/2$

$f_{bl}(p,q)=f(i,j)$ $\quad N/2+1 \leq i \leq N/2$

$1 \leq j \leq N/2$

$f_{br}(p,q)=f(i,j)$ $\quad N/2+1 \leq i \leq N/2$

$N/2+1 \leq j \leq N/2$

Where $1 \le p \le N/2$, $1 \le q \le N/2$.

3. Block based SVD Transformation is applied on f_{tl} (p,q), $1 \le p \le N/2$ and $1 \le q \le N/2$ with a block size of M*M.

4.2 Watermark Embedding in D Matrix:

Bin no.	$\mathbf{d_{low}}$	$\mathbf{d_{high}}$
1	d_{min}-T	d_{min}
2	d_{min}	d_{min}+T
3	d_{min}+T	d_{min}+2T
..	..	..
..	..	..
b_{n-1}	d_{max}-T	d_{max}
b_n	d_{max}	d_{max+}T

Table 1: Quantization table for the largest singular values

4. From each block of D matrix, obtain the largest coefficient D(1,1). From these D(1,1)'s, a matrix D_{large} is formed. The size of D_{large} is, same as that of watermark image.

5. The entire range d_{min} (minimum value of D_{large}) to d_{max} (maximum value of D_{large}) is divided into various bins as shown in above table. A step size of T is taken as the difference from one bin to another bin.

6. Each element of D_{large} matrix is checked for its position in the table.

After identifying the bin number, D_{large} is modified as follows

1. If watermark bit is 1 then it belongs to Range1, where Range1 is defined as

$$Range\ 1 = d_{low}(n) \ to \ \frac{d_{low}(n) + d_{high}(n)}{2}$$

D_{large} is modified as

$$D_{large} = \frac{d_{low}(n) + \dfrac{d_{low}(n) + d_{high}(n)}{2}}{2}$$

2. If watermark bit is 1 then it belongs to Range1, where Range1 is defined as

$$Range\ 2 = \frac{d_{low}(n) + d_{high}(n)}{2} \ to \ d_{low}(n)$$

D_{large} is modified as

$$D_{large} = \frac{d_{high}(n) + \frac{d_{low}(n) + d_{high}(n)}{2}}{2}$$

7. After the modification applied in the above step, inverse SVD is applied to get the first portion of the watermatked image $f_{tlw}(p,q)$.

The above steps are repeated for the second block $f_{tr}(p,q)$ to get watermarked image $f_{trw}(p,q)$.

Robustness of the method against attacks and imperceptibility of watermark image can be improved with the increase in the number of bins and the decrease in step size.

4.3 Watermark Embedding In U Matrix:

8. Block based SVD transformation is applied on sub image $f_{bl}(p,q)$, $1 \leq p \leq N/2$ and $1 \leq q \leq N/2$ with a block size of M*M.

9. Watermark image w (i,j), $1 \leq i \leq N/2M$ and $1 \leq j \leq N/2M$ is embedded in the columns of each block of U matrix, u_{11}(first row,first column) and u_{21}(second row first column) are modified as follows:

$$u_{diff} = |u_{11}| - |u_{21}|$$

If w (i,j)=1 and $u_{diff} > \alpha$

or

w (i,j)=0 and $u_{diff} < \alpha$

$$u_{11} = -\left|\,|u_{11}| + (\alpha - u_{diff})/2\,\right|$$

$$u_{21} = -\left|\,|u_{21}| - (\alpha - u_{diff})/2\,\right|$$

If w (i,j)=0 and $u_{diff} < \alpha$

or

w (i,j)=0 and $u_{diff} > \alpha$

$$u_{11} = -\left|\,|u_{11}| + (\alpha + u_{diff})/2\,\right|$$

$$u_{21} = -\left|\,|u_{21}| - (\alpha + u_{diff})/2\,\right|$$

Where '| |' indicates the absolute value. The above modification is applied to the coefficients of each block of u matrix. Here, α is a constant.

10. After the modification of U matrix coefficients, inverse SVD is applied to each block to get the second portion of the watermarked image $f_{blw}(p,q)$. The above steps are repeated for the next portion $f_{br}(p,q)$ to get the watermarked image $f_{brw}(p,q)$.

11. All the sub images $f_{tlw}(p,q)$, $f_{trw}(p,q)$, $f_{blw}(p,q)$, and $f_{brw}(p,q)$ are combined appropriately to get the final watermarked image F(i,j).

Flowchart for embedding scheme:

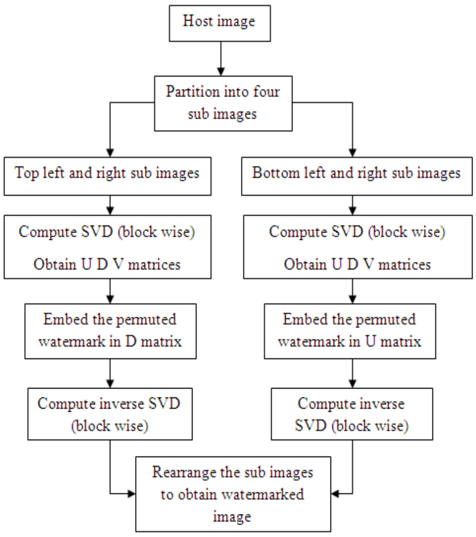


Fig 1: Flow chart for embedding scheme

4.4 Watermarked Image (F (i,j)) Partition:

1. The watermarked image F(i, j) of size N× N is partitioned into four quarters and four sub images $f_{tlw}(p,q)$ (top left watermarked), $f_{trw}(p,q)$ (top right watermarked) ,$f_{blw}(p,q)$ (bottom left watermarked) and $f_{brw}(p,q)$ (bottom right watermarked) are obtained.

4.5 Watermark Extraction from D Matrix:

2. SVD transformation is applied on top left portion $f_{tlw}(p,q)$.

3. From each block of D matrix obtained from SVD of $f_{tlw}(p,q)$, the largest coefficient D(1,1) is extracted.

4. The value of D (1,1) is checked for its positioning the quantization table. From this step, bin position is identified.

5. From the bin position obtained in step 4, now the D(1,1) value is checked for its position, Range1 or Range2. If it is in Range1, the watermark bit is '1' otherwise, the watermark bit is '0'.

Steps 1 to 5 is repeated for all the largest coefficients of all the blocks od D component. In this way, the watermark image of size N/2M*N/2M is extracted.

4.6 Watermark Extraction from U Matrix:

6. SVD transformation is applied on the watermarked sub image $f_{brw}(p,q)$.

7. Elements u_{11} and u_{21} of U matrix generated from the previous step are compared for generating watermark.

$$w(i,j)=0 \text{ if } |u_{11}| > |u_{21}| \quad \text{for } 1 \le i \le N/2,$$

$$1 \le j \le N/2$$

$$w(i,j)=1 \text{ otherwise.}$$

Flowchart for extracting watermark:

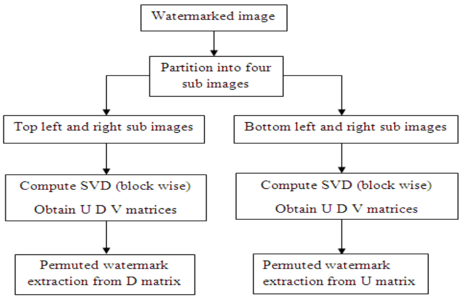
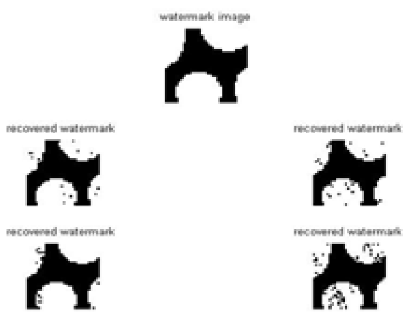


Fig 2: Flow chart for extraction of watermark

V. RESULTS

5.1 Original Image Watermark Image Watermarked Image

5.2 RECOVERED WATERMARK:



VI. CONCLUSION

In this paper, a robust watermarking scheme based on SVD is proposed. The watermark image is embedded in both D and U matrices. Since, the same watermark is embedded twice in the same image, the rate of watermark survival is high. Robustness is achieved by using the Dither quantization for D matrix and altering coefficients of U matrix. The quality of the watermarked image is good in terms of perceptibility and PSNR (45.5611 db).

REFERENCES

[1] I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing,* 6(12), 1673-1687, December, 1997.

[2] C.I.Podilchuk and E.J.Delp, "Digital Watermarking: Algorithms and Applications", *IEEE Signal Processing Magazine,* pp.33-46, July 2001.

[3] I.J.Cox, M.L.Miller, and J.A. Bloom, *Digital watermarking*, Morgan Kaufmann Publishers, San Francisco, CA, 2002.

[4] Tao Peining and Eskicioglu Ahmet M, "An Adaptive Method for Image Recovery in the DFT Domain", *Journal of Multimedia*, Vol.1, No.6, September 2006.

[5] Barni, F. Bartolini, A. Piva . "A DCT domain system for robust image watermarking", *IEEE Transactions on Signal Processing,* 66, 357-372, 1998.

[6] Chu, W.C, "DCT based image watermarking using sub sampling", *IEEE Trans Multimedia* 5, 34-38, 2003.

[7] M.Barni, M., Bartolini, F., V., Piva, A, "Improved wavelet based watermarking through pixel-wise masking," *IEEE Trans Image Processing* 10, 783-791, 2001.

[8] Y. Wang, J.F.Doherty and R.E.Van Dyck, "A wavelet based watermarking algorithm for ownership verification of digital images", *IEEE Transactions on Image Processing,* 11, No.2, pp.77-88, February 2002.

[9] V. I. Gorodetski, L. J. Popyack, V. Samoilov and V. A. Skormin, "SVD-based Approach to Transparent Embedding Data into Digital Images", *International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001),* St. Petersburg, Russia, May 21-23, 2001.

[10] R.Liu, T.Tan, "An SVD-based watermarking scheme for protecting rightful ownership", *IEEE Trans. Multimedia,* (4),1, pp, 121-128, 2002.

[11] D. V. S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition", *Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems,* Tulsa, OK, pp. 264-267, 2002.

[12] Sun, R., Sun, H., Yao, T, "A SVD and quantization based semi-fragile watermarking technique for image authentication" *Proc. IEEE International Conf. Signal Processing,* 2. 1592-95, 2002.

[13] Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, "SVD based digital image watermarking scheme". *Pattern Recognition Letters* 26, 1577-1586, 2005.

[14] S.Srinivas Kumar, B.Chandra Mohan and B.N.Chatterji, "An Oblivious Image Watermarking Scheme using Singular Value Decomposition," *IASTED International Conference on Signal and Image Processing (ICSIP'07),* Honolulu, Hawaii, USA, August 20-22, 2007.

[15] Chung K,Yang W ,Huang Y, Wu S, Hsu Yu-Chiao, "On SVD-based watermarking algorithm" *Applied Mathematics and Computation* Elsevier, 188, 54-57, 2007.

[16] E.Ganic and A.M.Eskiciougulu, "Secure DWT-SVD Domain Image Wtermarking: Embedding Data in All Frequencies", *ACM Multimedia and Security Workshop* 2004, Magdeburg, Germany, September 20-21, 2004.

[17] Jieh-Ming Shieh, Der-Chyuan Lou and Ming-Chang Chang, "A semi-blind digital watermarking scheme based on singular value decomposition", Computer Standards and Interfaces 28, 428-440, 2006.

[18] Ganic E, Zubair N, Eskicioglu AM. "An optimum watermarking scheme based on singular value decomposition", *International Conference on Communication Network and Information Security*, Uniondale, Ny, p.85-90, 2003.

[19] ZI-Quan Hong, "Algebraic Feature Extraction of image for recognition" *Pattern Recognition*, Vol.24, No.l3, pp.211-219, 1991.

[20] Brian Chen and G.W.Wornell, "Digital Watermarking and information embedding using dither modulation", *Proceedings of the IEEE workshop on Multimedia Signal Processing (MMSP-98),* Redondo Beach, CA, December 1998.

[21] Brian Chen and G.W.Wornell, "Preprocessed and postprocessed quantization index modulation methods for digital watermarking", *Proceedings of SPIE: Security and Watermarking of Multimedia Contents* II, Vol.3971,1999.

[22] http://www.morgan-multimedia.com