ROBUST WATERMARKING OF COLOR IMAGES USING SEGMENTATION AND DWT-SVD TRANSFORMATION

Divya Gautam[1] Ms. Sarika Khandelwal [2]
[123] *Department of Computer Engineering, Geetanjali Institute of Technical Studies,Udaipur*

Abstract— **Digital watermarking is a branch of information system security that finds tremendous applications in the modern era of internet and digital data exchange. Specifically, digital image watermarking finds vast applications in medical image processing, satellite images and related fields. In this paper, a blind and robust watermarking approach using DWT and SVD based transformations is presented. A given color image partitioned into RGB color planes and the entropy of each of the plane is computed for choosing the optimal plane for watermark embedding. The chosen plane is then segmented into non-overlapping blocks and watermarking bits are embedded into each of the blocks separately, considering the human visual system (HVS) characteristics based on the entropy values. For each of the block, the 2 level DWT is performed which transforms the image into four sub-bands namely HH, HL, LH and LL bands. Subsequently, Singular Value Decomposition (SVD) is performed on the HH band. The HH band is chosen to provide a robust watermarking as it contains most of the information contained in the original signal. Alternatively, LL band can be chosen to implement fragile watermarking scheme with a high PSNR values. To embed the watermark bits, the U and V matrix values are suitably modified to embed a zero or one. As compared to the S matrix of SVD transform, the embedding of the watermarking bits into the U and V singular matrices gives a much robust watermarking with low false positive rate and hence, are preferred when robustness is critical issue. The proposed technique is compared with those proposed by Nasrin M. et.al. and the simulation results established that better robustness and imperceptibility is achieved as indicated through PSNR.**

Keywords— **Discrete Wavelet Transform, Singular Value Decomposition, Image Entropy, Human Visual System etc.**

I. INTRODUCTION

In Watermarking a message related to the verifiable content of the digital signal is shielded and hidden inside the cover media. Watermarking has been used for several centuries, in different forms like in initial level watermarks found in plain paper and subsequently in paper bills. Nevertheless, digital watermarking is the technology that was only developed during the last 15 years and it is now being used for many different applications. The increasing amount of research on watermarking over the past decade [2] has been largely driven by its important applications in digital copyrights management and protection.

Every watermarking system has some very important advisable properties. There are some conflicting properties and depending on the application of the watermarking system there are some tradeoffs between these properties which we are often forced to accept. The first and one of the most important property is effectiveness. This property refers to the need that the message in a watermarked image will be correctly detected. This probability is ideally needed to be 1. The second important property is the image fidelity. Watermarking is a process that changes an original image to add a message to it, therefore it inevitably affects the image's quality. This degradation of the image's quality must be kept to a minimum, so that no obvious difference in the image fidelity is percepted by Human Eye [3]. The third property is the payload size. Watermarking is basically used to carry a message and for this size of the message is very important as because for embedding it in a cover work many systems require a relatively big payload. The fourth and another important property is the false positive rate to watermarking systems. It directs to the number of digital works that are discovered to have a watermark embedded when there is no watermark embedded. And it should be kept very low for watermarking systems. Lastly, robustness is another very important property for most watermarking systems. There are many situations in which a watermarked image is altered during its lifetime, by several malicious attacks that try to remove the watermark or make it undetectable or either by transmission over a lossy channel. A robust watermark should be able to confront additive Gaussian noise, printing and scanning, compression, rotation, scaling, cropping and several other operations. Figure 1.1 shows a generic architecture of a watermarking system.

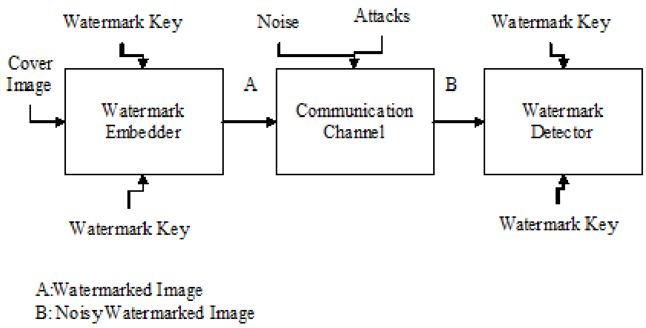


Fig 1.1 Generic Watermarking System

Watermarking Application Areas

One of the first and important application for watermarking was broadcast monitoring [4]. It is often critically important that we are able to track when a specific video is being broadcast by a TV station. This property is important to advertising agencies because they want to ensure that whether their commercials are getting the air time they paid for. Watermarking is beneficial for this purpose. With the help of watermarking information used to identify individual videos could be embedded in the videos themselves making broadcast monitoring easier. The third and very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is also a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or song, one could use watermarking to embed the copyright in the image or the song itself. Transaction tracking is another interesting application of watermarking [5]. In this case the watermark embedded in a digital work can be used to record one or more transactions taking place in the history of a copy of this work. For example, watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each copy. If the movie is then leaked to the Internet, the movie producers could identify which recipient of the movie was the source of the leak.

Finally, copy control [6] is a very promising application for watermarking. In this application, watermarking can be used to prevent the illegal copying of songs, images of movies, by embedding a watermark in them that would instruct a watermarking-compatible DVD or CD writer to not write the song or movie because it is an illegal copy.

Problem Statement

In this paper a technique of watermarking of digital images is presented which is robust for geometrical attacks [7]. These geometrical attacks include rotation, scaling and translation attacks. The robustness for geometrical attacks is achieved by computing the invariant moments [8] of the cover image. These invariants are a set of numeric values which remains the same for the image if it is rotated, scaled or translated in some direction. The invariance of these values towards cropping is achieved by considering the invariant moments of the part of the image which has the least probability of coming under cropping operation in some image processing operation. These invariant moments are embedded redundantly in the image to achieve a robust watermarking. The embedding is done using standard Singular Value Decomposition (SVD) [9, 10] based matrix decomposition of the image and the watermark is embedded in the S matrix of the image. This provides the best results considering the quality of the watermark image, as the watermarking information is ideally distributed throughout all the pixels of the image providing better image quality and robustness at the same time. The proposed technique provides a way for blind watermarking in which the original unmarked image is not required at the receiver end for watermark extraction.

Section 1 presents an overview of the subject matter and gives the problem statement and the approach for the research. Section 2 provides the motivation and research approach to the subject. It also makes a background for the concepts and techniques presented in subsequent Sections. Section 3 and Section 4 presents the proposed model for comparison of an incoming bug report with positive and negative examples. Section 5 gives the simulation results and the plots for various features for similarity measurement. Section 6 concludes the paper and provides an insight for future prospective of the work.

II. RESEARCH APPROACH AND MOTIVATION

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. The protection and enforcement of intellectual property rights for digital media have become an important issue. Digital watermarking is that technology that provides and ensures security, data authentication and copyright protection to the digital media. Digital watermarking is the embedding of signal or secret information into the digital media such as image, audio and video. Later the embedded information is detected and extracted out to reveal the real owner/identity of the digital media. Watermarking is used for following reasons, Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication, Data Hiding. Watermarking consists of two modules watermark embedding module and watermark detection and extraction module. Digital watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and label of the user information.

Research Approach

The image is first operated to find out the invariant moments of the image segment which is least prone to be subjected to cropping operation. These are the numeric values which remain the same even if the image is rotated, scaled or translated. The textual watermark is encoded in binary and the XORed with the normalized values of invariant moments and embedded in the coefficients of the S matrix of the SVD decomposition. This process can be performed repeatedly for non overlapping segments of the image to provide a robust watermarking which is robust against cropping operations on the image. At the receiving end, invariant moments of the image are computed and operated on the segments of the cover image to extract the watermark.

III. PROPOSED WATERMARKING SCHEME

3.1 Proposed Watermarking Scheme

The proposed watermarking scheme embeds a binary image watermark into the host image. The embedding process is implemented by segmenting the image into non-overlapping blocks and embedding a binary bit into each of the blocks. Thus, if the given color cover image has a dimension of NXN, an embedding capacity of NXN/(kXk) can be achieved, where k is the size of the image segment. In the proposed watermarking scheme, blue color plane is considered for watermark embedding as the human eye has least perceptiveness for blue color as compared to Red and Green Color. This results into robust watermarking scheme considering the perceptual characteristics of the human visual system.

To implement a blind watermarking scheme, provision are needed to be inculcated at the receiver end that the watermark can be extracted/ detected without the need of original unmarked file at the recover. In fact, the receiver is not supposed to be provided with any kind of key or cue to facilitate the detection and/or extraction of the watermark. However, such a scheme can be implemented using custom watermarks or watermarks generated from the feature vectors of the image, considering only those features only that remain unchanged before and after the watermarking process. In the proposed scheme, custom watermark are used and the same is extracted at the receiver. It is important to note that almost all the blind watermarking schemes that are proposed in literature makes use of the (invariant) features of the original image in one form or other. In the proposed work, the watermarking is performed on the Blue color plane using features that are generated from Red and Green Planes.

3.1.1 Image Features used for watermark embedding

The noise in the image can be computed in several ways. It represents the extent of disturbances in the intensity of different regions on the image. Passion, Gaussian, Impulse, Salt and Pepper are the common noise variants. In this paper, Noise Value Function is used for noise representation. The NVF is implemented using sliding window the minimum size of which is 3. Thus for any pixel P(i,j) in the original image, there is a pixel P'(i,j) in the NVF image which is obtained using arithmetic operations on the image segment of size 9X9 centered over the image. For all the nine pixels in the segment, the average is computed, then the value of the difference of the average and the original pixel is computed. The same is assigned to P'(i,j). The window moves a pixel further from left to right to compute the same process. It is important to note that for boundary nodes, only the nodes that actually covered by the window is considered. The resultant pixel values are again subjected to an operation so as to make the difference lie in the range 0-255. In this paper, generalized scaling is done after the computation of all the NVF values of the image. The NVF computation is done for the pixels of the RED and GREEN color plane.

The NVF computation is pictorially depicted as shown :

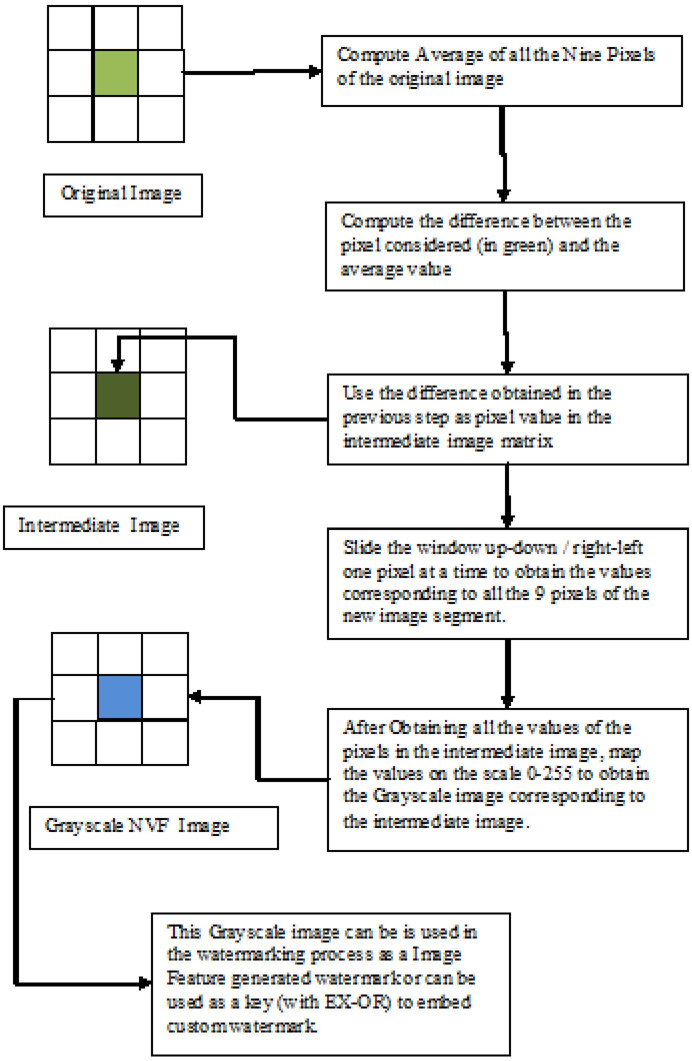


Fig 3.1 Feature Vector Computation

3.1.1 Generation of the watermark

The watermark generation is done using the NVF values of the image color plane. It is the necessary condition for the watermark generation that it is generated from those features of the image that remain invariant before and after the watermarking process.

1. Consider original Image (I_{MxM}) and decompose it into Red, Green and Blue Channels.
2. Any of the plane, either the Red or Green, may be computed for the computation for the generation of watermark.
3. The chosen color plane represents a matrix, the elements of which are on the scale from 0-255. There are several functions that can be used to model noise in an image.
4. Compute the NVF (Noise Visibility Function) of the image using the method described above. By applying the NVF, the watermark in the texture and border becomes stronger than in flat areas.
5. Reduce the size of the NVF to I_{MxM} /(4X4) by averaging operation.
6. Obtain the Binary matrix corresponding to the grayscale NVF matrix using mapping to 0,1 of the values of the grayscale NVF image.
7. For a given custom binary watermark of size I/(4X4), obtain the pair-wise Ex-OR operation on the two matrices.
8. Embed the bits of the matrix so obtained in the SVD decomposition of HH band of 4X4 block of Blue Plane of the Original Image as per the proposed scheme.

3.1.2 Watermarking Scheme

The proposed watermarking scheme is based on the following schematic to implement a robust blind watermarking scheme:

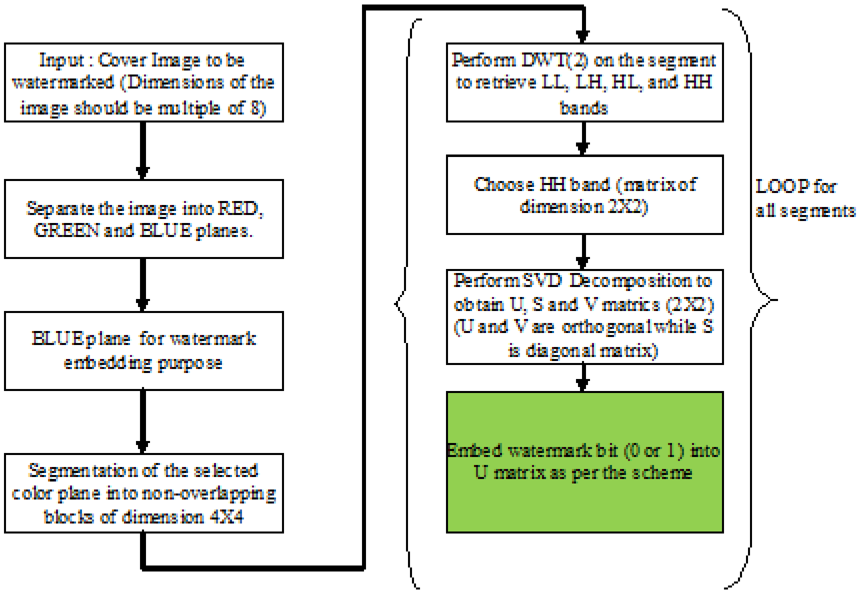


Fig 3.2 Schematic of the proposed watermarking scheme

The figure 3.1 shown above shows the steps involved in the proposed watermarking scheme in a broad manner. The operation indicated in green color block holds the major details of the watermarking scheme and can be altered to implement a robust or fragile watermarking scheme. It is important to note that in the SVD decomposition of the matrix, a given matrix S is split into three matrices U, S and V, in such a way as to satisfy the following equation :

$$S = U * S * V^T$$

Here, both U and V are orthogonal matrices and S is a diagonal matrix. It is important to note that an orthogonal matrix is one for which the determinant is ±1. Embedding the watermark into the U or V matrix is done in a suitable way to maintain the visual characteristics of the image.

The following numerical relationships hold for dimensions of the Image as well as watermark:

TABLE 3.1
PARAMETER SPECIFICATIONS

S. No.	Object	Specification	Remarks
1	Original Image Dimension	NXN	Pixel Matrix N must be a multiple of 8
2	Original Image /Blue Plane Segment Dimension	8X8	Pixel Matrix having values in the range 0-255 Each Segment holds on Pixel of watermark image.
3	HH Band of Segment	4X4	Real Values
4	SVD Decomposition U, S and V matrices of HH	4X4 Each	Real Values Embedding takes place on this 4X4 block
5	NVF Image Generation from RED/ GREEN Plane	NXN	Pixel Matrix
6	NVF Image Normalization	NXN	Pixel Matrix in the range (0-255)
7	NVF Averaging over non overlapping block of size 8X8	NXN/(8X8)	Pixel Matrix in the range (0-255)
8	NVF Conversion to Binary Image	NXN/(8X8)	Binary Matrix (0,1)
9	Custom Watermark	NXN/(8X8)	Binary Matrix (0,1)
10	Embedding Binary Matrix	NXN/(8X8)	Binary Matrix (0,1) Obtained as a result of Exclusive-OR Operation of 8 and 9 objects

3.2 SVD Decomposition

Singular Value Decomposition is a factorization of any m*n matrix I in USV^T matrix, where U is a m*m unitary matrix and V is n*n unitary matrix and S is the m*n rectangular diagonal matrix in which all except the diagonal elements are zero.

$I = USV^T$

The singular values in the S matrix consist of values of large magnitude and the magnitude decrease rapidly with row order. These higher magnitude S matrix diagonal elements consist of most of the information about the original matrix. The U and V matrices, on the other hand, consists of very low magnitude values as compared to the values in the S matrix and thus consists of lesser information. The watermarking scheme proposed in this paper can be more appropriately understood by analyzing the consequences of matrix manipulation over its SVD decomposition.

The advantages and disadvantages of the SVD decomposition are as given below:

Advantages of SVD decomposition

1. SVD decomposition of a matrix is a very powerful technique in matrix decomposition and analysis.
2. SVD is more robust to the numerical error in matrix computation.

3. SVD decomposition gives the geometric structure of a matrix which is the important aspect of any matrix calculation.

Disadvantages of SVD decomposition

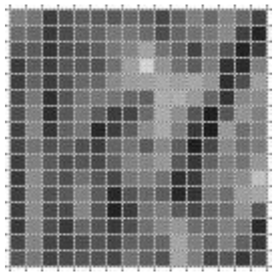
1. There are some drawbacks of using SVD decomposition for the problems which can be solved by other simpler techniques such as Fourier transformations etc. because SVD decompositions make the problem computationally complex.
2. SVD is not susceptible to problems that require flexible algorithms because it operates on fixed matrix.

An image can be thought of as a pixel grid or more appropriately, a matrix of real numbers. In figure 3.3, a sample color image is shown and a corresponding grayscale image is also shown. The grayscale image can be obtained as the linear sum of all the three, viz; red, green and blue color planes.

Lena Color Image (64X64) jpg

Lena grayscale Image (64X64) jpg

Lena grayscale Image (32X32) jpg



Lena grayscale Image (16X16) jpg (magnified 800 percent)

Sample Image: Dimension 4X4 (magnified 800 percent)

Fig. 3.3 Sample color and grayscale Images

The corresponding matrix for grayscale image is shown in table 3.2

TABLE 3.2
MATRIX CORRESPONDING TO THE GRAYSCALE IMAGE SHOWN IN FIG 3.1 (16X16)

122	111	61	88	94	95	99	92	92	90	88	120	114	133	100	76
123	108	51	83	94	96	113	121	109	82	100	117	120	131	71	29
84	91	49	82	88	87	117	146	168	108	94	78	106	88	37	58
58	95	60	83	84	82	121	163	196	156	109	93	129	47	35	135
64	109	60	78	99	108	137	161	149	175	163	169	158	45	82	156
72	113	53	84	123	119	109	103	112	165	176	161	94	57	139	137
78	118	60	95	121	84	61	64	123	164	148	86	31	89	148	125
76	120	65	95	105	55	61	107	133	173	132	50	50	139	117	114
69	120	85	92	76	62	95	129	91	144	87	37	72	138	113	126
60	133	89	82	84	79	99	125	134	139	97	61	99	136	113	154
55	140	87	82	108	90	80	107	129	105	58	58	120	123	140	182
56	141	82	91	132	89	46	81	112	103	35	54	121	112	173	158
57	141	76	82	129	85	35	68	106	123	83	66	104	103	147	81
60	140	72	63	104	86	55	77	108	134	160	113	103	135	121	58
69	132	69	61	89	84	74	94	96	103	168	134	86	128	90	63
80	123	68	74	90	78	77	103	105	93	145	137	70	91	63	57

TABLE 3.3
U MATRIX (FROM SVD DECOMPOSITION) CORRESPONDING TO THE MATRIX SHOWN IN FIG 3.3

-0.23794	-0.04148	0.186602	-0.34537	0.205842	0.199112	-0.3785	-0.02464	0.274481	-0.41542	-0.33156	0.189677	-0.38126	0.074209	0.110365	-0.06932
-0.23413	-0.22397	0.203613	-0.49582	0.068505	-0.02329	-0.27242	-0.15822	0.029487	0.104553	0.186833	-0.34556	0.466213	-0.13476	-0.30457	0.094046

-0.22879	-0.28601	-0.19183	-0.30801	-0.19743	-0.37507	-0.11186	0.072032	0.00778	0.469713	0.135883	0.236186	-0.18529	0.066881	0.438992	-0.10181
-0.25846	-0.31556	-0.50941	0.044587	-0.12106	-0.28468	0.121302	0.092003	0.050427	-0.22789	-0.24849	-0.0204	-0.07449	0.216792	-0.51801	0.125443
-0.29871	-0.38453	-0.25811	0.291501	0.288199	0.191369	0.11643	-0.31058	-0.02379	-0.2598	0.132242	-0.15857	0.22477	-0.00996	0.441523	-0.15925
-0.28289	-0.14709	0.111816	0.472891	0.269239	0.13004	-0.30585	-0.08968	-0.03795	0.394551	0.132556	0.208082	-0.28787	-0.21527	-0.32583	0.133642
-0.25026	0.170039	0.167279	0.418844	-0.21035	-0.18009	-0.42508	0.266673	0.133273	0.056729	-0.29228	-0.2227	0.331381	0.274038	0.176736	-0.06639
-0.2513	0.177935	0.036786	0.114734	-0.55607	-0.08699	-0.08434	-0.11045	0.169295	-0.39332	0.521178	0.016868	-0.15677	-0.27218	-0.0248	-0.00563
-0.23808	0.204297	-0.12506	-0.11386	-0.3521	0.452637	-0.06816	-0.34277	-0.48588	0.132653	-0.10805	-0.01447	-0.06226	0.353387	0.00804	0.16613
-0.26233	0.161079	-0.20774	-0.07416	-0.17103	0.301468	0.185709	0.093669	0.182037	0.189306	-0.34451	0.234596	0.270533	-0.50144	-0.07707	-0.34629
-0.25766	0.326979	-0.27775	-0.1102	0.225326	0.166304	0.128994	0.356081	0.209379	0.143236	0.130819	-0.48437	-0.24541	-0.06547	0.145667	0.337244
-0.24502	0.469007	-0.15053	-0.08817	0.396133	-0.1797	-0.02363	0.062661	-0.1073	-0.11588	0.304799	0.460707	0.297376	0.256186	-0.08638	-0.06516
-0.23115	0.277655	0.138503	-0.01395	0.162444	-0.48148	0.135169	-0.30342	-0.34958	-0.01449	-0.25302	-0.30827	-0.25138	-0.23725	-0.01278	-0.28362
-0.24866	0.01703	0.372778	0.039845	-0.03623	-0.14149	0.47291	-0.28892	0.329906	0.079372	-0.17267	0.201419	0.113555	0.084517	0.108757	0.501486
-0.23886	-0.12959	0.367018	-0.00816	-0.03097	0.190691	0.384455	0.221243	0.078788	0.102336	0.216685	-0.11852	-0.15332	0.40113	-0.20072	-0.5049
-0.22392	-0.21892	0.259833	-0.02442	-0.02678	0.025459	0.11971	0.539828	-0.55762	-0.24183	-0.04096	0.135383	0.065578	-0.24221	0.118699	0.245432

TABLE 3.4
S-MATRIX (FROM SVD DECOMPOSITION) CORRESPONDING TO THE MATRIX SHOWN IN FIG 3.3

1634.219	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	268.8938	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	219.3403	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	187.458	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	147.5803	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	95.74478	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	89.57724	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	56.83706	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	37.64654	0	0	0	0	0	0	0

0	0	0	0	0	0	0	0	0	31.92614	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	20.80309	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	6.063212	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	4.259442	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	3.486705	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.56473	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.119327

TABLE 3.5

V MATRIX (FROM SVD DECOMPOSITION) CORRESPONDING TO THE MATRIX SHOWN IN FIG 3.3

-0.1791	-0.09278	0.187371	-0.30162	-0.05475	0.021177	-0.57814	0.0682	0.087574	-0.36707	-0.12584	-0.42212	0.183072	0.032835	0.141943	-0.31578
-0.29484	0.198708	0.159042	-0.10207	0.026564	-0.04973	0.332039	0.212578	-0.34246	-0.01011	-0.20185	-0.39323	0.168212	-0.33335	-0.46416	0.107851
-0.16565	0.152874	-0.00272	-0.09144	-0.03643	0.11031	0.263595	0.146748	-0.36557	-0.03734	-0.51021	0.153894	-0.07899	0.190924	0.600378	-0.11888
-0.20064	0.074588	-0.02097	-0.07739	-0.10081	-0.09972	-0.32885	0.048073	-0.30769	-0.19701	-0.05394	0.255949	-0.20173	0.543209	-0.37867	0.368952
-0.24761	0.145418	0.114781	0.044365	0.159737	-0.4175	-0.16058	0.059855	-0.17995	0.038524	0.40611	-0.1547	-0.40319	-0.26136	0.400163	0.243897
-0.21172	-0.06507	0.057838	-0.02845	0.271955	-0.07624	-0.13755	0.039016	0.065619	0.496793	-0.20719	0.057174	-0.4541	0.50111	-0.26324	-0.52083
-0.21268	-0.30217	-0.19331	-0.15281	-0.01588	0.336038	-0.28553	-0.07119	0.028121	0.477112	-0.22634	-0.07715	0.088464	-0.19648	0.122678	0.50585
-0.26752	-0.24664	-0.31577	-0.207	-0.19093	0.145535	0.078712	-0.10034	-0.46562	0.086835	0.518028	0.090466	0.168586	0.013937	-0.00471	-0.34874
-0.30118	-0.13607	-0.30832	-0.05635	-0.21161	-0.58587	0.084968	0.374372	0.359336	0.061792	-0.09843	0.188501	0.279082	0.013486	0.029889	-0.00393
-0.31779	0.00769	-0.10128	0.387729	-0.35555	-0.09065	-0.06833	-0.58277	0.007481	-0.22925	-0.26098	0.101426	-0.12959	-0.31567	-0.05626	-0.09393
-0.28391	-0.3206	0.40353	0.413626	-0.26188	0.103993	0.23252	0.060376	0.12671	0.142854	0.139042	-0.32269	-0.02101	0.420478	0.076689	0.05034
-0.23679	-0.42179	0.314529	0.144436	0.420284	0.159103	0.002358	0.196841	-0.0179	-0.32088	0.020343	0.476592	0.097957	-0.25268	-0.02492	0.025054
-0.24261	-0.11989	-0.19217	-0.29729	0.49447	-0.10304	0.340589	-0.46876	0.211831	-0.19697	-0.01511	-0.20121	-0.02108	0.26931	0.020883	0.113179
-0.25539	0.284711	0.292277	-0.48626	-0.33026	0.279656	0.167651	-0.0107	0.395689	-0.02346	0.17766	0.255998	-0.21874	-0.10983	-0.01856	0.043243
-0.25876	0.513044	0.200432	0.18159	0.235501	-0.00385	-0.18245	-0.21638	0.021418	0.283029	0.104328	0.177335	0.557292	0.145287	0.0664	-0.04591
-0.26636	0.295883	-0.5059	0.334702	0.152259	0.429324	-0.04568	0.342381	0.21213	-0.20565	0.112018	-0.14864	-0.15053	0.021711	-0.01775	-0.0368

It is easy to verify that the determinant of both U and V matrices is 1 and hence these are orthogonal. Also, it can be verified that

$$I = U * S * V^T$$

It is the property of SVD decomposition of the matrices that the U and V matrices remain almost unchanged with the change in values of the individual pixels, up to some extent like in the LSB encoding. However, singular matrix S consists of values which are large in order of magnitude as compared to the elements of other matrices and thus change proportionately to the magnitude. These singular values consist of most of the information about the image and can be encoded in a suitable way for watermarking purpose so as to provide a way of blind watermarking technique. However, in this paper, an approach is presented to embed the watermark in the U and V matrices of the SVD decomposition.

Consider the fifth image of figure 3.1. The image matrix I and the corresponding U, S and V matrices are as shown:

$$I = \begin{bmatrix} 94 & 104 & 133 & 88 \\ 86 & 91 & 132 & 108 \\ 102 & 75 & 93 & 114 \\ 89 & 86 & 105 & 103 \end{bmatrix}$$

$$U = \begin{bmatrix} -0.5226 & -0.6008 & -0.5743 & -0.1898 \\ -0.5232 & -0.2323 & -0.7908 & -0.2166 \\ -0.4756 & -0.7459 & -0.2097 & -0.4165 \\ -0.4762 & -0.1697 & -0.0290 & -0.8623 \end{bmatrix}$$

$$S = \begin{bmatrix} 403.3442 & 0 & 0 & 0 \\ 0 & 39.2140 & 0 & 0 \\ 0 & 0 & 15.1039 & 0 \\ 0 & 0 & 0 & 4.7504 \end{bmatrix}$$

$$V = \begin{bmatrix} -0.4587 & 0.3757 & 0.6587 & -0.4632 \\ -0.4428 & -0.3336 & 0.3965 & 0.7317 \\ -0.5772 & -0.5962 & -0.3611 & -0.4255 \\ -0.5102 & 0.6262 & -0.5278 & 0.2627 \end{bmatrix}$$

It is clearly evident that the U and V matrices consists of low magnitude values whereas the S matrix consists of Singular values which have high magnitude and drops exponentially as the row count increases.

The SVD watermarking in U and V matrices can be illustrated by taking the example of a 4 X 4 matrix as shown:

$$A = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{bmatrix} \begin{bmatrix} b_1 & 0 & 0 & 0 \\ 0 & b_2 & 0 & 0 \\ 0 & 0 & b_3 & 0 \\ 0 & 0 & 0 & b_4 \end{bmatrix} \begin{bmatrix} c_1 & c_5 & c_9 & c_{13} \\ c_2 & c_6 & c_{10} & c_{14} \\ c_3 & c_7 & c_{11} & c_{15} \\ c_4 & c_8 & c_{12} & c_{16} \end{bmatrix}$$

Thus

$$\begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{bmatrix} = \begin{bmatrix} a_1b_1 & a_2b_2 & a_3b_3 & a_4b_4 \\ a_5b_1 & a_6b_2 & a_7b_3 & a_8b_4 \\ a_9b_1 & a_{10}b_2 & a_{11}b_3 & a_{12}b_4 \\ a_{13}b_1 & a_{14}b_2 & a_{15}b_3 & a_{16}b_4 \end{bmatrix} \begin{bmatrix} c_1 & c_5 & c_9 & c_{13} \\ c_2 & c_6 & c_{10} & c_{14} \\ c_3 & c_7 & c_{11} & c_{15} \\ c_4 & c_8 & c_{12} & c_{16} \end{bmatrix}$$

Further simplification yields

$$\left[\underbrace{\begin{matrix} a_1b_1c_1 + a_2b_2c_2 + a_3b_3c_3 + a_4b_4c_4 & a_1b_1c_5 + a_2b_2c_6 + a_3b_3c_7 + a_4b_4c_8 \\ a_5b_1c_1 + a_6b_2c_2 + a_7b_3c_3 + a_8b_4c_4 & a_5b_1c_5 + a_6b_2c_6 + a_7b_3c_7 + a_8b_4c_8 \\ a_9b_1c_1 + a_{10}b_2c_2 + a_{11}b_3c_3 + a_{12}b_4c_4 & a_9b_1c_5 + a_{10}b_2c_6 + a_{11}b_3c_7 + a_{12}b_4c_8 \\ a_{13}b_1c_1 + a_{14}b_2c_2 + a_{15}b_3c_3 + a_{16}b_4c_4 & a_{13}b_1c_5 + a_{14}b_2c_6 + a_{15}b_3c_7 + a_{16}b_4c_8 \end{matrix}}_{\text{First Two Columns of Resultant Matrix}}\right]$$

3.3 Proposed SVD Based Embedding Scheme

Consider a sample hypothetical image matrix of dimension 2X2 as shown:

$$A = \begin{bmatrix} 23 & 34 \\ 56 & 78 \end{bmatrix}$$

In this paper work, the embedding is performed on 2X2 matrix and hence the mathematical properties of the same are explored in subsequent sections. The SVD decomposition of the given A matrix is:

$$U = \begin{bmatrix} -0.392996119057335 & -0.919540129850717 \\ -0.919540129850717 & 0.392996119057335 \end{bmatrix}$$

$$S = \begin{bmatrix} 104.421694605656 & 0 \\ 0 & 1.05342094298900 \end{bmatrix}$$

$$V = \begin{bmatrix} -0.579699058117757 & 0.814830658491312 \\ -0.814830658491312 & -0.579699058117757 \end{bmatrix}$$

It can be easily verified that the determinant of U matrix is -1 and that of V matrix is 1. Also it is important to note that both U and V matrices are of the form:

$$U = \begin{bmatrix} -a & -b \\ -b & a \end{bmatrix}$$

$$V = \begin{bmatrix} -c & d \\ -d & -c \end{bmatrix}$$

where a, b, c and d are real positive numbers.

Also

$$|U| = -a^2 - b^2 = -1$$

Similarly

$$|V| = c^2 + d^2 = 1$$

It is important to note that the SVD decomposition of any matrix S yields the matrices U, S and V, in which the U and V matrices are orthogonal whereas the S is a diagonal matrix. For any given matrix, the S matrix is unique. However, the U and V matrices are not unique and one can suitably change the values of elements in U and V matrices to embed the hidden data. For any matrix of dimension 2X2, the U and V matrices consists of values that satisfied the relationship given above.

It is clear that the absolute value of the elements of the U matrix, a and b satisfied the relationship that the sum of square of both a and b is 1. Thus, we can find angle in the range

$$[-\frac{\pi}{2},\frac{\pi}{2}]$$

where

$$\mathrm{Sin}\theta = \frac{a}{\sqrt{a^2+b^2}}$$

and

$$\mathrm{Cos}\theta = \frac{b}{\sqrt{a^2+b^2}}$$

Considering the embedding in U matrix, let α and β be two variable such that

$$U' = \begin{bmatrix} -(a-\alpha) & -(b-\beta) \\ -(b-\beta) & (a-\alpha) \end{bmatrix}$$

To keep the orthogonality property unchanged, it is required that

$$|U'| = -(a-\alpha)^2 - (b-\beta)^2 = -1$$
$$(a-\alpha)^2 + (b-\beta)^2 = 1$$
$$a^2 + \alpha^2 - 2a\alpha + b^2 + \beta^2 - 2b\beta = 1$$
$$\alpha^2 + \beta^2 - 2(b\beta + a\alpha) = 0$$
$$\alpha^2 - 2a\alpha - (2b\beta - \beta^2) = 0$$
$$\alpha = \frac{2a \pm \sqrt{4a^2 + 4(2b\beta - \beta^2)}}{2}$$

The two values of α corresponding to the solution of the above quadratic equation can be computed as a function of the values of parameter β. The embedding of the watermark in the 4X4 matrix can be done as per the scheme of watermark embedding.

Larger values of the parameter α and β gives robust watermarking and smaller values provide fragile watermarking. At the same time, larger values corresponds to small PSNR and vice versa.

Thus, both the values needs to be chosen appropriately to provide a robust watermarking scheme, while at the same time, with an acceptable PSNR.

The significance of the modification of the values of a and b as per the embedding of the watermark bit is shown in figure 3.4.

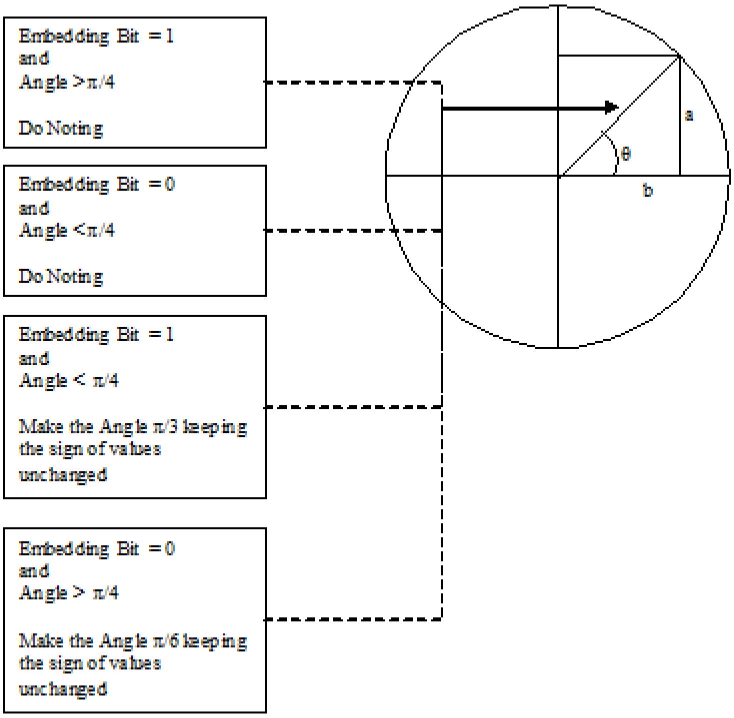


Fig 3.4 Embedding Scheme for Watermarking Bits

The values of the matrix elements can be directly obtained by setting the angle values and finding the corresponding sine and cosine values. Section 4 gives the simulation results for the watermarking scheme developed in this Section.

network so as to achieve maximum network lifetime.

IV. RESULTS

4.1 Image DWT Computation

The DWT Transform of a matrix takes the following form:

Consider a hypothetical image (I) of dimension 4X4, represented in matrix form as shown:

I =

TABLE 4.1

IMAGE MATRIX OF HYPOTHETICAL IMAGE (I)

22	21	42	48
24	23	41	28
35	24	37	37
25	53	39	28

The Discrete Wavelet Transform of the Hypothetical image is as shown:

TABLE 4.2

DWT TRANSFORM OF THE HYPOTETICAL MATRIX

HL=

-2	10.5
-9.5	3.5

HH=

45	79.5
68.5	70.5

LH =

1	3.5
-8.5	5.5

LL=

-1.22E-15	-9.5
19.5	-5.5

As stated in the Section 3, to implement robust watermarking, HH band is used for watermark embedding. However, to implement fragile watermarking, LL band can be used for watermark embedding.

In the proposed work watermarking is implanted on the HH band of the DWT transform of the 4X4 segments of the Blue color plane of the watermark.

The image used for watermark embedding illustration is shown in figure 4.1

Fig 4.1 Original Squirrel Image - Dimension (400X400)

The separation of the given image into RED, GREEN and BLUE color planes is depicted in figure 4.2,4.3 and 4.4 respectively.

Fig 4.2 RED Color Plane

Fig 4.3 GREEN Color Plane

Fig 4.4 BLUE Color Plane

4.2 Generation of the Watermark

As state in Section 3, the red or the green color planes are used for NVF Generation and the Blue Plane is used for watermark embedding. This is because the human eye is least susceptible for blue color. In this simulation, the GREEN color plane is chosen for watermark embedding. The computation of NVF function first performs averaging using a sliding window scheme. The window, typically of size 3X3, 5X5 etc., is positioned over the image and moved horizontally and vertically one pixel at a time. The pixel value is replaced by the average value of pixels in the window. The averaging operation of a sliding window, centered at a pixel is shown for the GREEN color image plane. It is important to note that all the R, G and B planes consists of values in the range 0-255. Taken individually, these represents the grayscale color values. The subsequent image represents the grayscale versions of the GREEN color plane chosen for NVF Generation. Fig 4.5, 4.6, 4.7 and 4.8 shows the variations in the image as the size of the sliding window increases.

Fig 4.5 Mean Value Approximation using sliding Window : Window size 3X3

Fig 4.6 Mean Value Approximation using sliding Window : Window size 5X5

Fig 4.7 Mean Value Approximation using sliding Window : Window size 9X9

Fig 4.8 Mean Value Approximation using sliding Window : Window size 20X20

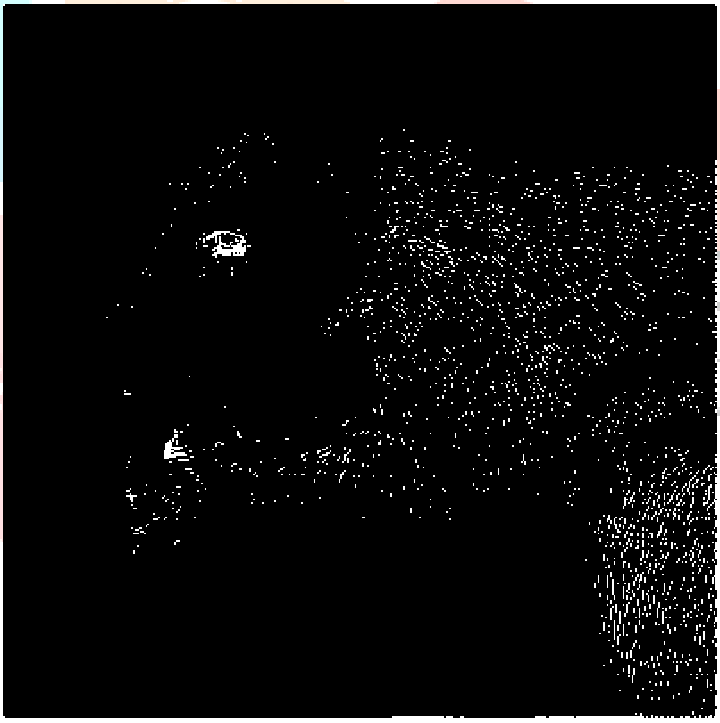


Fig 4.9 Visualization of the NVF image corresponding to the GREEN plane approximated by window size 3X3.

Fig 4.10 Visualization of the NVF image using block averaging of 4X4 non overlapping block

The copyright image used in the simulation is shown in figure 411

Fig 4.11 Copyright Image: To be embedded : Original Dimension 100X100

It is important to note that both Fig 4.10 and 4.11 are converted to binary images using the mapping procedure of grayscale image pixel values to {0,1}. Generally, the pixel values below 125 are mapped to 0 and 126 to 255 are mapped to 1. The watermark image to be embedded in the Blue color plane of the cover image is obtained using the EX-Or Operation bitwise on the pixels of images 4.10 and 4.11 The resultant binary image is shown in figure 4.12

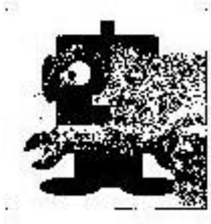


Figure 4.12 Ex-Or of Copyright and NVF Image

This is important to note that the image shown in figure 4.12 is obtained as a result of Ex-OR operation (bitwise) on two matrices of dimension 100X100. If any one of the matrix, either copyright or NVF is again ex-order with this image, the other one is obtained. In proposed scheme, the NVF image is generated from the GREEN color plane which remains unchanged in the watermarking process. Thus, NVF is obtained at the receiver end and when it is operated with the extracted binary pattern, givens the watermark image.

4.3 Watermarking Process

Watermarking is done on non overlapping blocks of size 4x4 of the original image. The subsequent figures shows the stepwise simulation output of the proposed watermarking process. The block of the specified size is processed iteratively and the HH band is used for watermark embedding as per the proposed scheme.

Figure 4.13 Watermarked Binary Image Blue Plane- Shown in Grayscale Color-map

Figure 4.14 Watermarked Binary Image Blue Plane

Figure 4.14 Watermarked Color Image : Obtained after combining RED, GREEN and Watermarked BLUE Plane

4.4 Comparison of the Proposed Work with the Base Work

It is evident through perceptiveness that the proposed techniques perform well over the color images. However, the Quality Metric of the watermarking process has always been the Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE).

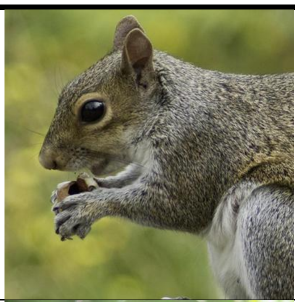
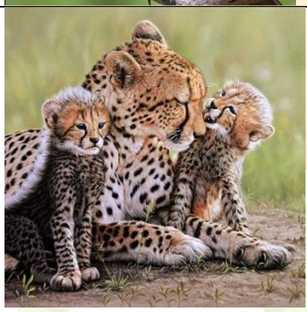
The MSE is defined as the mean value of the sum of square of the differences between the watermarked image and the original image, hence termed as Mean Square Error. The PSNR and the MSE are related with each other in the following way.

$$\text{PSNR} = 10\, log_{10} \frac{Max\ Value * Max\ Value}{MSE}$$

The MSE and PSNR values of the sample images is tabulated as shown :

TABLE 4.3
PSNR AND MSE VALUES OF THE SAMPLE IMAGES

S. No.	Image	Quality Index (Proposed)	Base Work Nasrin M et al [6]
1		MSE = 0.1121	MSE = 0.2123

		PSNR = 57.63dB	PSNR = 54.86dB
2		MSE = 0.5763	MSE = 0.6152
		PSNR = 50.52dB	PSNR = 50.24dB
3		MSE = 0.3457	MSE = 0.4551
		PSNR = 52.74dB	PSNR = 51.54dB
4		MSE = 0.4376	MSE = 0.4784
		PSNR = 51.72dB	PSNR = 51.33dB

The graphical illustration for MSE and PSNR between the proposed and the base approach is shown in subsequent graphs.

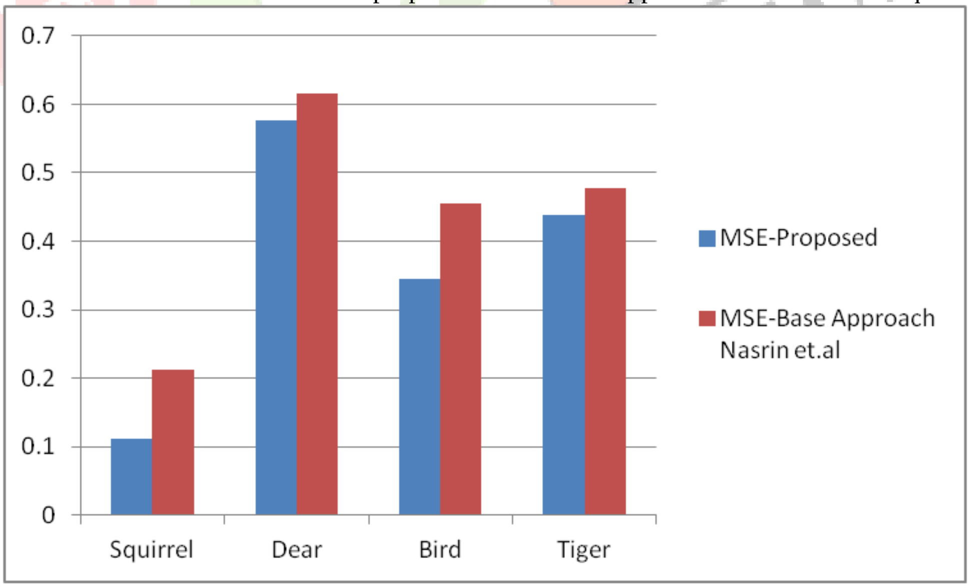


Figure 4.15 Comparison of the MSE values

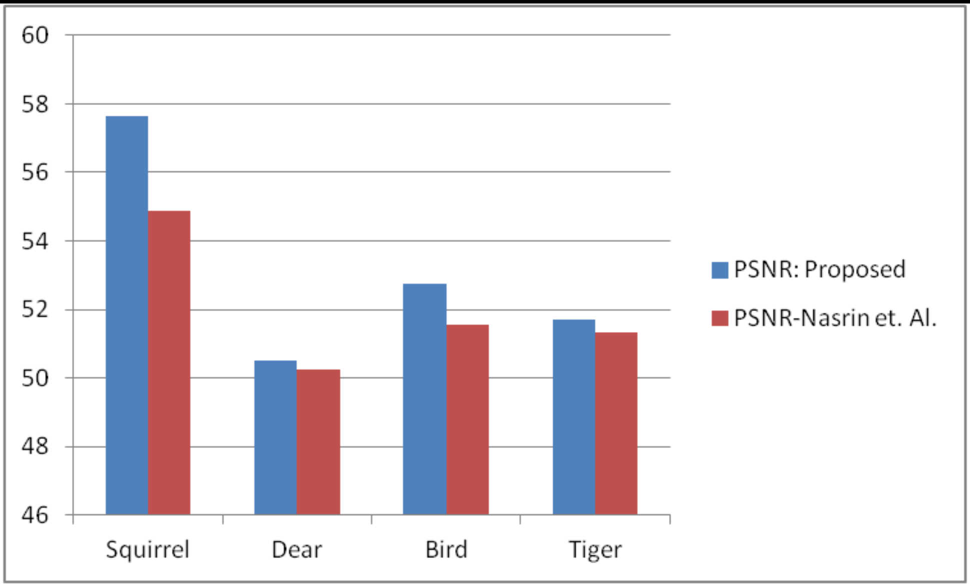


Figure 4.15 Comparison of the PSNR values

It is evident that the proposed technique outperforms that of the approach proposed by Nasrin et.al. Also, the proposed technique embeds the watermark in the HH band thereby implementing a robust watermarking scheme resistant to several kind of attacks. Section 5 concludes the paper and gives the scope for future work.

V. CONCLUSION

A robust watermarking scheme is presented using the combination of techniques which are predominant in the watermarking processes of digital images. In the proposed scheme, based on human perceptiveness values, the blue color plane is used for watermark embedding. As the proposed scheme is blind, a feature vector needs to be generated from the original image. In this paper, the NVF image is used as the feature vector and custom watermark is embedded using the ex-or operation of NVF matrix with the chosen watermark.

The watermark is embedded bit by bit into the HH matrix of the non overlapping segments of the image. The proposed scheme outperforms as proposed in the base research work. However, a main reason for obtaining better PSNR level is the low embedding capacity, as compared to the other techniques like LSB and DFT. The comparison of the results proves the effectiveness of the proposed technique as compared tp the base approach.

As the future scope of this work, a DWT-SVD based watermarking approach is to be formulated which is resistant to attacks like jpg compression and print and scan attacks. Moreover, the watermarking techniques needs to be semi fragile as per the need of time, so that it can provide tempering protection and at the same time, used for embedding the watermark so robustly that no attacker can destroy or remove the watermark. Another aspect of the future work is to improve the embedding capacity of the scheme. Moreover, the current technique embeds the watermark in U matrix of the SVD decomposition. As a future aspect, of this work, the watermark is to embedded in the matrices much more evenly so as to provide better perceptual quality of the watermarked image..

REFERENCES

[1] Thangadurai, K.; Sudha Devi, G., "An analysis of LSB based image steganography techniques," in Computer Communication and Informatics (ICCCI), 2014 International Conference on , vol., no., pp.1-4, 3-5 Jan. 2014 doi: 10.1109/ICCCI.2014.6921751

[2] Prabhishek Singh, R S Chadha ,"A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013

[3] Macq, B.; Dittmann, J.; Delp, E.J., "Benchmarking of image watermarking algorithms for digital rights management," in Proceedings of the IEEE , vol.92, no.6, pp.971-984, June 2004 doi: 10.1109/JPROC.2004.827361

[4] Li Liu; Xiaoju Li, "Watermarking Protocol for Broadcast Monitoring," in E-Business and E-Government (ICEE), 2010 International Conference on , vol., no., pp.1634-1637, 7-9 May 2010 doi: 10.1109/ICEE.2010.414

[5] Emmanuel, S.; Vinod, A.P.; Rajan, D.; Heng, C.K., "An Authentication Watermarking Scheme with Transaction Tracking Enabled," in Digital EcoSystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES , vol., no., pp.481-486, 21-23 Feb. 2007 doi: 10.1109/DEST.2007.372024

[6] Petrovic, R.; Tehranchi, B.; Winograd, J.M., "Security of Copy-Control Watermarks," in Telecommunications in Modern Satellite, Cable and Broadcasting Services, 2007. TELSIKS 2007. 8th International Conference on , vol., no., pp.117-126, 26-28 Sept. 2007 doi: 10.1109/TELSKS.2007.4375954

[7] Liang, Liu; Qi, Sun, "Robust image watermarking against geometrical attacks," in Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on , vol., no., pp.1-3, 6-9 Nov. 2006

[8] Ruliang Zhang; Lin Wang, "An image matching evolutionary algorithm based on Hu invariant moments," in Image Analysis and Signal Processing (IASP), 2011 International Conference on , vol., no., pp.113-117, 21-23 Oct. 2011 doi: 10.1109/IASP.2011.6109009

[9] Makhloghi, M.; Akhlaghian, F.; Danyali, H., "Robust digital image watermarking using singular value decomposition," in Signal Processing and Information Technology (ISSPIT), 2010 IEEE International Symposium on , vol., no., pp.219-224, 15-18 Dec. 2010 doi: 10.1109/ISSPIT.2010.5711780

[10] Smitha Rao M.S, Jyothsna A.N, Pinaka Pani.R," Digital Watermarking: Applications, Techniques and Attacks ", International Journal of Computer Applications (0975 – 8887) Volume 44– No.7, April 2012

[11] Gregg, D.M.; Blackert, W.J.; Heinbuch, D.V.; Furnanage, D., "Assessing and quantifying denial of service attacks," in Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE , vol.1, no., pp.76-80 vol.1, 2001 doi: 10.1109/MILCOM.2001.985767

[12] IEEE Standard Specifications for Password-Based Public-Key Cryptographic Techniques," in IEEE Std 1363.2-2008 , vol., no., pp.1-127, Jan. 29 2009 doi: 10.1109/IEEESTD.2009.4773330

[13] Chaudhary, A.; Ahmad, K.; Rizvi, M.A., "E-Commerce Security through Asymmetric Key Algorithm," in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, vol., no., pp.776-781, 7-9 April 2014 doi: 10.1109/CSNT.2014.163

[14] Smid, M.E.; Branstad, D.K., "Data Encryption Standard: past and future," in Proceedings of the IEEE , vol.76, no.5, pp.550-559, May 1988 doi: 10.1109/5.4441

[15] Sowmya Nag, K.; Bhuvaneswari, H.B.; Nuthan, A.C., "Implementation of advanced encryption Standard-192 bit using multiple keys," in Research & Technology in the Coming Decades (CRT 2013), National Conference on Challenges in , vol., no., pp.1-7, 27-28 Sept. 2013 doi: 10.1049/cp.2013.2514

[16] Chu-Hsing Lin; Chen-Yu Lee; Yi-Shiung Yeh; Hung-Sheng Chien; Shih-Pei Chien, "Generalized secure hash algorithm: SHA-X," in EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE , vol., no., pp.1-4, 27-29 April 2011 doi: 10.1109/EUROCON.2011.5929187

[17] Warner, M., "Notes on the Evolution of Computer Security Policy in the US Government, 1965-2003," in Annals of the History of Computing, IEEE , vol.37, no.2, pp.8-18, Apr.-June 2015 doi: 10.1109/MAHC.2015.25

[18] Chen Hai-peng; Shen Xuan-jing; Wei Wei, "Digital Signature Algorithm Based on Hash Round Function and Self-Certified Public Key System," in Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on , vol.2, no., pp.618-624, 7-8 March 2009 doi: 10.1109/ETCS.2009.399

[19] Ragab, A.H.M.; Ismail, N.A.; Allah, O.S.F., "An efficient message digest algorithm (MD) for data security," in TENCON 2001. Proceedings of IEEE Region 10 International Conference on Electrical and Electronic Technology , vol.1, no., pp.191-197 vol.1, 2001 doi: 10.1109/TENCON.2001.949578

[20] Thangadurai, K.; Sudha Devi, G., "An analysis of LSB based image steganography techniques," in Computer Communication and Informatics (ICCCI), 2014 International Conference on , vol., no., pp.1-4, 3-5 Jan. 2014 doi: 10.1109/ICCCI.2014.6921751

[21] Bouchama, S.; Aliane, H.; Hamami, L., "Watermarking Techniques Applied to H264/AVC Video Standard," in Information Science and Applications (ICISA), 2010 International Conference on , vol., no., pp.1-7, 21-23 April 2010 doi: 10.1109/ICISA.2010.5480288

[22] Clarke, R.J., "Video coding: an introduction to standard codecs [Book Review]," in Computing & Control Engineering Journal , vol.11, no.4, pp.204-204, Aug 2000

[23] Chauhan, S.P.S.; Rizvi, S.A.M., "A survey: Digital audio watermarking techniques and applications," in Computer and Communication Technology (ICCCT), 2013 4th International Conference on , vol., no., pp.185-192, 20-22 Sept. 2013 doi: 10.1109/ICCCT.2013.6749625

[24] Koizumi, T.; Mori, M.; Taniguchi, S., "Speech recognition based on a model of human auditory system," in Spoken Language, 1996. ICSLP 96. Proceedings., Fourth International Conference on , vol.2, no., pp.937-940 vol.2, 3-6 Oct 1996 doi: 10.1109/ICSLP.1996.607756

[25] Chun-Hsiang Huang; Ja-Ling Wu,, "Attacking visible watermarking schemes," in Multimedia, IEEE Transactions on , vol.6, no.1, pp.16-30, Feb. 2004 doi: 10.1109/TMM.2003.819579

[26] Xiaodong Deng; Mengtian Rong; Tao Liu; Yong Yuan; Dan Yu, "Segmented Cyclic Redundancy Check: A Data Protection Scheme for Fast Reading RFID Tag's Memory," in Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE , vol., no., pp.1576-1581, March 31 2008-April 3 2008 doi: 10.1109/WCNC.2008.282

[27] Singh, A.K.; Sharma, N.; Dave, M.; Mohan, A., "A novel technique for digital image watermarking in spatial domain," in Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on , vol., no., pp.497-501, 6-8 Dec. 2012 doi: 10.1109/PDGC.2012.6449871

[28] Tirkel, A., Rankin, G., Schyndel, R. V., Ho, W., Mee, N., AND Osborne, C. 1993. Electronic watermark. In Proceedings of DICTA. 666–672.

[29] Kurah, C. AND Mchughes, J. 1992. A cautionary note on image downgrading. In Proceedings of the IEEE Computer Security Applications Conference. Vol. 2. IEEE Computer Society Press, Los Alamitos, CA,153–159.

[30] Yadav, N.; Singh, K., "Transform domain robust image-adaptive watermarking: Prevalent techniques and their evaluation," in Computing, Communication & Automation (ICCCA), 2015 International Conference on , vol., no., pp.1121-1126, 15-16 May 2015 doi: 10.1109/CCAA.2015.7148543

[31] Chi-Man Pun, "A Novel DFT-based Digital Watermarking System for Images," in Signal Processing, 2006 8th International Conference on , vol.2, no., pp., 16-20 2006 doi: 10.1109/ICOSP.2006.345581

[32] Chu, W.C., "DCT-based image watermarking using subsampling," in Multimedia, IEEE Transactions on , vol.5, no.1, pp.34-38, March 2003 doi: 10.1109/TMM.2003.808816

[33] Shih, F.Y.; Yi-Ta Wu, "A novel fragile watermarking technique," in Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on , vol.2, no., pp.875-878 Vol.2, 30-30 June 2004
doi: 10.1109/ICME.2004.1394340

[34] Yang, S.Y.; Lu, Z.D.; Zou, F.H., "A novel semi-fragile watermarking technique for image authentication," in Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on , vol.3, no., pp.2282-2285 vol.3, 31 Aug.-4 Sept. 2004
doi: 10.1109/ICOSP.2004.1442235

[35] Jun Xiao; Zhiqiang Ma; Bai Lin; Jiaorao Su; Ying Wang, "A semi-fragile watermarking distinguishing JPEG compression and gray-scale-transformation from malicious manipulation," in Information Computing and Telecommunications (YC-ICT), 2010 IEEE Youth Conference on , vol., no., pp.202-205, 28-30 Nov. 2010
doi: 10.1109/YCICT.2010.5713080

[36] Imran, M.; Ghafoor, A.; Khokher, M.R., "A robust non-blind color image watermarking scheme," in Control Automation Robotics & Vision (ICARCV), 2012 12th International Conference on , vol., no., pp.1392-1396, 5-7 Dec. 2012
doi: 10.1109/ICARCV.2012.6485392

[37] Pradhan, C.; Saha, B.J.; Kabi, K.K.; Arun; Bisoi, A.K., "Blind watermarking techniques using DCT and arnold 2D cat map for color images," in Communications and Signal Processing (ICCSP), 2014 International Conference on , vol., no., pp.026-030, 3-5 April 2014
doi: 10.1109/ICCSP.2014.6949772

[38] Hae-Kwang Kim; Jong-Deuk Kim; Dong-Gyu Sim; Dae-Il Oh, "A modified Zernike moment shape descriptor invariant to translation, rotation and scale for similarity-based image retrieval," in Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on , vol.1, no., pp.307-310 vol.1, 2000
doi: 10.1109/ICME.2000.869602

[39] Ye Xueyi, Deng Meng, Wang Yunlu, Zhang Jing, "A Robust DWT-SVD Blind Watermarking algorithm Based on Zernike Moments", Communications Security Conference (CSC 2014), 2014 Pages: 1 - 6,
DOI: 10.1049/cp.2014.0734