ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

A Study on Reversible Fragile Image Watermarking Scheme

Pooja Loni[1], V.S. Malemath[1], Sushma Chaugule[1], Anup Kalyanashetti[2]

Department of CSE, KLE Dr.MSS College of Engg. & Tech. Belgaum[1]

Department of CSE, AMC Engineering College, Bangalore[2]

Abstract: Digital watermarking is the way that is used to protect the confidential information in the form of images from the hackers or intruders. Images like medical images, military images contain vital information they must be protected from modification and attacks. Irreversible watermarking schemes have various limitations such as permanent embedding distortion. The problem of the embedding capacity depends on signal, that is the capacity of embedding depends on nature of the host signal and the block-wise dependence problem were not addressed by the researches of reversible watermarking schemes. This work proposes a reversible watermarking scheme which reduces the discussed limitations of irreversible and reversible schemes with different parameters.

Keywords: Fragile; Watermark; Reversible; Embed; Extract.

I. INTRODUCTION

The process of hiding digital information for achieving legitimacy is called "watermarking". Nowadays with coming technology, datasets and images are produced by different modalities. The images or file should be protected from unauthorized use. Digital watermarking is used to show the identity of its owner and confirm the legitimacy or integrity. The basic idea behind watermarking is to hide or embed a secrete image or information into an original image so that it can be retrieved later by extraction and protect against the attacks. The original image can be recovered from the watermarked image completely.

Recent researchers have made great effort into the study of fragile watermarking methods for multimedia and image authentication. (Perrig et al.)[1] And others [2-5] have stated that "Permanent embedding distortion is the limitation of all irreversible watermarking schemes", to recover the original signal it cannot be erased after the signal passing through the authentication procedure.(C. W. Honsinger et al.) [6] Have tried to resolve this problem. Low embedding capacity and Salt and pepper artifacts owing to intensity wraparound (e.g., intensity change from 0 to 255 or vice versa for 8-bit images) can be resolved.

Vector quantization is a classical quantization technique from signal processing which allows the modeling of probability density functions by the distribution of prototype vectors. A reversible watermarking scheme with near constant signal-independent embedding capacity and immunity to the vector quantization attack and transplantation attack is proposed here.

It is originally used for data compression. A large set of points (vectors) are divided into groups having approximately the same number of points closest to them. Its centroid point is used to represent each group, as in k-means and some other clustering algorithms like Centroid based, Distribution based, Density based clustering algorithms.

Transplantation attack which is another form of malicious operation of collecting blocks to create a counterfeit.
Considering the problem definitions here is the brief description of the proposed scheme i.e. read an image which is called watermark image and embed it into the original image(as shown in the figure) whose transformation is authenticated. Embedding algorithm is used for this process.

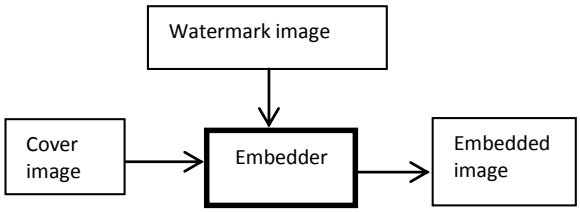


Fig.1.1 Processing at sender side (embedding).

At the receiver end we extract the watermark image from embedded cover image (as shown in the fig below). Extraction algorithm is used for this process.

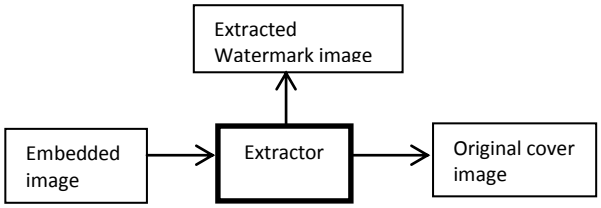


Fig. 1.2. Processing at receiver side (extraction).

The feature of this scheme is that it is very efficient in terms of high embedding capacity with low distortion and also eliminates vector quantization attack and transplantation attack and is reversible.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

II. LITERATURE REVIEW

In the recent past, researchers have made major efforts investigating digital watermarking schemes to meet the needs of copyright protection and authentication of multimedia. Usually the schemes for copyright protection are robust and fragile. Robust in the sense, it is strong enough to withstand the manipulation and the embedded watermark can still be preserved. Fragile means delicate, that is when attacked entire embedded watermark should be destroyed and the alarm should be raised when the extracted watermark is wrong [2].

(Chang and Yinyin, p.13-14) have devised a digital watermarking scheme with watermark embedding and detection algorithms which can resist to cut and paste, Holliman memon counterfeit and transplantation attack. They offered a post processing scheme for enhancing localization resolution without affecting the security.

By varying the size of neighborhood and number of watermark able bits, the balance between security tamper localization and embedding distortion is adjusted.
Narawade et al. 2011, p.47-49) have reported that the increase in embedding capacity decreases the PSNR value and vice versa. Following are the technique of reversible watermarking scheme.

i) Data hiding using Integer Wavelet Transform,
ii) Histogram bin Shifting,
iii) Difference Expansion
iv) Contrast Mapping, and
v) Integer Discrete Cosine Transform. [15]

Savakar and Ghuli, [14] have proposed watermark insertion and extraction methodologies using haar wavelets in watermark image and devised that DWT, Chirp-Z and Fast Walsh-Hadamard Transforms can be used in digital watermarks.

Barton [12] proposed one of the earliest reversible data embedding schemes, which compress the bits to be affected by the embedding operation for two purposes: 1) creating space for the payload - the secret information to be hidden and 2) preserving the original data. The compressed data and the payload are then embedded into the host media. This practice of compressing original data for reversibility purpose has been widely adopted. (Honsinger et al.) [6] employed reversible embedding for authentication application, which uses addition modulo 256 to overcome the problems of overflow and underflow due to embedding operation.

Zeki et.al. [17] have carried out comparative study on steganographic software. Here they used one watermark image to be embedded within a different host images using five different software. Embedding in spatial domain is easier and simple where the image is directly embedded into a host by changing the position of pixel. Whereas in transform domain the host signal is transformed to desired domain before embedding. PSNR value is used to show the betterment in the performance of the software.

III. PROPOSED METHOD

In this work we propose two algorithms namely watermark embedding and watermark extraction. The image is read and converted into grayscale. Secrete information is calculated using neighborhood pixels as shown below.

25	63	253	200	245
23	152	245	54	12
69	120	145	11	74
23	20	251	124	23
56	85	88	95	65

Fig. 3.1 showing matrix representation of pixels

The pixel represented in red color is the pixel whose secrete information is to be calculated by using the neighborhood pixels, by adding all these neighborhood pixels which are in green color and dividing it by 256.by doing this for all the m*n pixels we get the secret information.

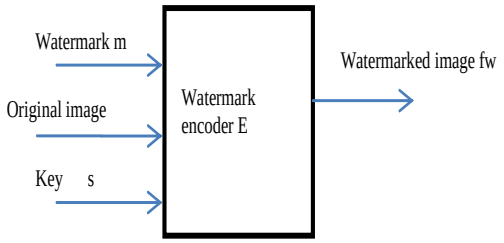


Fig. 3.2. Generic diagram for embedding algorithm:

The fig 3.2 shows the block diagram of embedding algorithm, we first select an image (Co) that is to be embedded with a watermark image m). Then calculate the secret information(s) using the original over image that is to be shared with the detector. Applying embedding algorithm we embed watermark to the original image and get the embedded (watermarked) image C'.

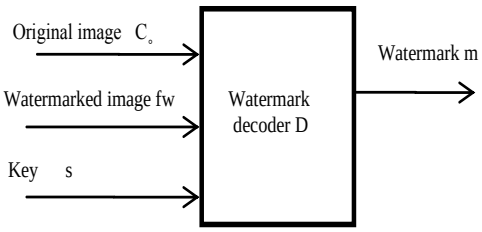


Fig.3.3. Block diagram of Generic watermark decoder

As shown in the diagram, select the same watermark image and initialize that to the extracted watermark w`. Perform the same operation as we did in embedding with the watermarked image C'. Using the secret key from the embedding part for extracting the watermark .Then if any pixel of the watermark and extracted watermark are same then we negate that pixel of embedded image to recover the original cover image.

DOI 10.17148/IJARCCE.2015.4894

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Mean filtering is easy to implement. It is used as a method of smoothing images, reducing the amount of intensity variation between one pixel and the next resulting in reducing noise in images.
Image filtering can be grouped in two depending on the effects:

1. Low pass filters (Smoothing)
2. High pass filters (Edge Detection, Sharpening)

Erosion is one of the two basic operators in the area of mathematical morphology, the other being dilation. It is typically applied to binary images, but there are versions that work on grayscale images. The basic effect of the operator on a binary image is to erode away the boundaries of regions of foreground pixels (i.e. white pixels, typically).

IV. ALGORITHMS

Algorithm: Watermark embedding algorithm
Input: 8-bit watermark image and cover image.
Output: watermarked image

Step 1: 8-bit watermark picture m is chosen.
Step 2: For every pixel i,
Step 2.1: Calculate the Hamming code h(C(i), m(i)).
Step 2.2: Calculate separation D(C(i), m(i))
Step 2.3: Negate the LSB of C(i) if D(C(i), m(i)) = 0 or 8 (preprocessing).
Step 3: Watermarkable pixels to be distinguished
Step 4: For each watermarkable pixel i,
Step 4.1: Calculate the secret data s(i) as per Eq. S(i)= ∑ j=N(i)mod 256 . s(i) is the secret key imparted to the finder.
Step 4.2: Negate the watermarkable bit of C(i).[16][18].

Algorithm: Watermark extraction algorithm
Input: watermarked image.
Output: Recovered cover image and extracted watermark.

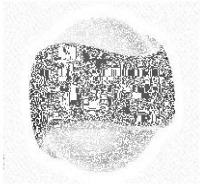
Step 1: Read a 8-bit watermark picture m with the secret key imparted to the embedder.
Step 2: Initialise the removed watermark m′ by letting m′ = m.
Step 3: For every pixel i, compute the Hamming code h(C′(i), m(i)) and separation D(C′(i), m(i))
Step 4: Identify watermarkable pixels
Step 5: For each watermarkable pixel i,
Step 5.1: Calculate the secret data s(i) indicated by Eq. (2)
Step 5.2: Extract watermark bit by setting m′j (i) = sj(i)
Step 5.3: Recover unique picture pixel C (i) by invalidating the watermarkable bit of C′(i) if m′(i) = m(i).
Step 6: Apply filters if necessary to remove noise from extracted watermark.

V. EXPERIMENTAL RESULTS

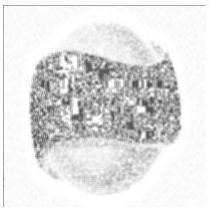
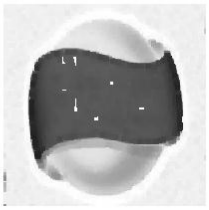
Experiment was conducted considering set of 50 images. In order to test the robustness of the algorithm a set of standard images such as Lena, baboons etc of different sizes were considered. The experimental results are encouraging and are shown in table 5.1-5.9.
Lena image (size 204:204)


Original cover image embedded image

Fig.4.1. Resulting images after applying Embedding algorithm

Watermark image Extracted watermark

After applying filter Eroded image

Recovered image

Fig.4.2. Resulting images after applying Extraction algorithm

TABLE I. Observations for Cover image and watermarked image using embedding algorithm with varying sizes.

Lena.jpg (size)	PSNR	AAD	NMSE
(204*204)	44.5843	0.6281	0.0111
(256*256)	44.7364	0.6267	0.0110
(300*300)	44.4383	0.6173	0.0108
(356*356)	44.6448	0.6224	0.0109
(400*400)	44.5869	0.6258	0.0110

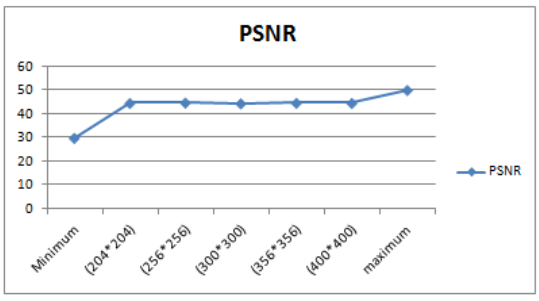


Fig.4.3. Peak Signal to Noise Ratio

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

As shown in the table 1 and graph 1 above the PSNR value for an image with different sizes using the same watermark image is approximately same, as the standard value for PSNR is 30-50 DB. The horizontal line in the graph shows that the PSNR value hardly changed for the change in the size of an image.

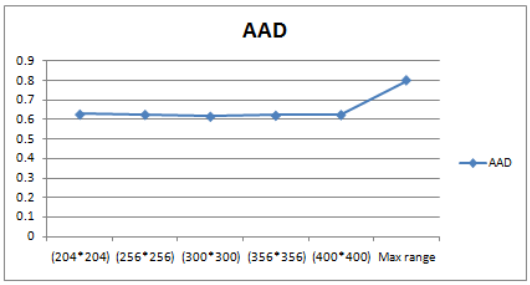


Fig.4.4. Average Absolute Difference

The Average Absolute Difference shows that two images have least difference. As listed in the table 1 above the AAD value is approximately same for all the different size images that is, 0.62. The graph 2 indicates there is no much difference in the AAD value if the size of the image is changed.

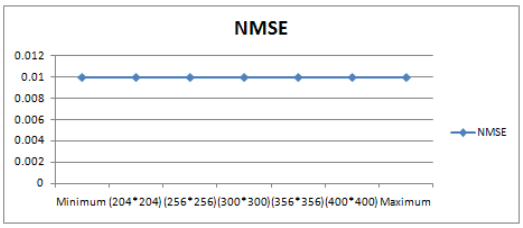


Fig.4.5. Normalized Mean Square Errors.

If a model has a very low NMSE value, then it is well performing in both time and space. In the table 1 and graph 3 we can observe that the NMSE value is very low with average of 0.01.

TABLE .II Observations for watermark image and extracted water mark image using Extraction algorithm.

.	MSE	NCC	SC	SC (Filter)	SC (Eroded)
(204*204)	1.3687	1	0.7521	0.7630	1.1059
(256*256)	1.3389	1	0.7525	0.7612	1.0.338
(300*300)	1.3035	1	0.7526	0.7600	1.0702
(356*356)	1.3246	1	0.7532	0.7594	1.0552
(400*400)	1.3364	1	0.7524	0.7579	1.0436

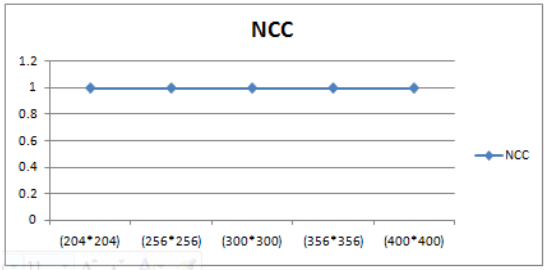


Fig.4.6. Normalize Cross Correlation.

Normalized Cross Correlation shows the correlation between two images, watermark and extracted watermark image, if the NCC value is 1; it shows that the two images are highly correlated. As we can observe in the table 2 and the graph 4 above that the NCC value for images regardless of its size, the value remains same i.e. 1 even if the filter and erosion is applied.

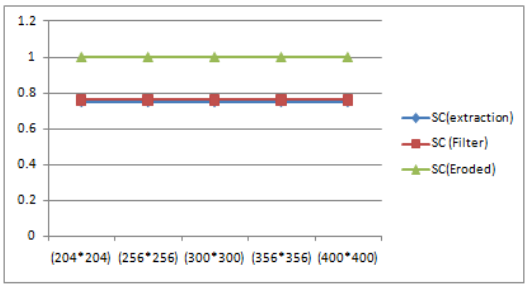


Fig4.7. Structural Content of watermark and Extracted watermark.

Structural content shows that the images are structurally Correlated.SC value 1 indicates that the images are highly correlated. As shown in the above graph the SC value for watermark and extracted watermark is approximately 0.75 (indicated by blue horizontal line), Brown line in the graph indicates the SC value of watermark and extracted watermark after applying filter with the value 0.76, which shows a slight improvement, and the green line illustrates that the images are highly correlated with the SC value=1 for different image sizes when erosion is applied.

TABLE .III Observations for Recovered and Original cover image.

Lena.jpg (size)	NCC	SC
(204*204)	1	1.0000
(256*256)	1	1.0000
(300*300)	1	0.9999
(356*356)	1	1.000
(400*400)	1	0.9999

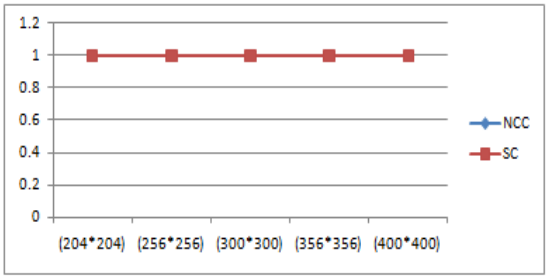


Fig. 4.8. Structural Content of watermark and Extracted watermark.

The above Graph illustrates the change in size of images will not matter for the NCC and SC of the recovered and Original image , the straight line indicates that the NCC and SC values are always 1 regardless of the size of the images.

DOI 10.17148/IJARCCE.2015.4894

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

TABLE .IV Observations for Cover image and watermarked image using embedding algorithm with varying Types.

Filenames with type	PSNR	AAD	NMSE
Lena.jpg	44.5843	0.6281	0.0111
Lena.tif	44.5843	0.6281	0.0111
Lena.bmp	44.5843	0.6281	0.0111
Lena.gif	44.5843	0.6281	0.0111

The tables below show that this model is applicable to all the image types like, Jpeg, Bitmap, tif etc. Regardless of the types of images the values for all the measures remain same.

TABLE .V Observations for watermark image and extracted water mark image using Extraction algorithm for varying image types (size 204*204).

Filenames with type	MSE	NCC	SC	SC Filter	SC Eroded
Lena.jpg	1.3687	1	0.7521	0.7630	1.1059
Lena.tif	1.3687	1	0.7521	0.7630	1.1059
Lena.bmp	1.3687	1	0.7521	0.7630	1.1059
Lena.gif	1.3687	1	0.7521	0.7630	1.1059

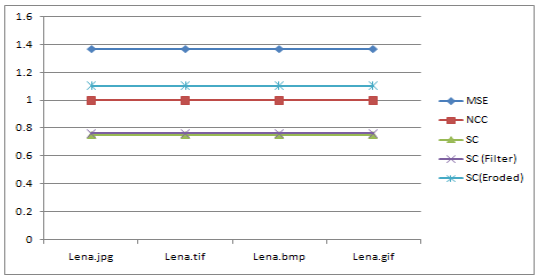


Fig. 4.9. Graph shows MSE, NCC, SC with and without filter for different images.

TABLE .VI Observations for Recovered and Original cover image.

Filenames with type	NCC	SC
Lena.jpg	1	1
Lena.tif	1	1
Lena.bmp	1	1
Lena.gif	1	1

TABLE .VII Observations for Cover image and watermarked image using embedding algorithm for different images.

Images	PSNR	AAD	NMSE
Fish.jpg	44.7801	0.6368	0.0110
Kat.jpg	45.1326	0.6367	0.0120
Mario.jpg	50.000	0.8610	0.0158
Dog.jpg	45.2598	0.6504	0.0119
Chick.jpg	44.6386	0.6205	0.0108

TABLE .VIII Observations for watermark image and extracted water mark image using Extraction algorithm for different images.

File names	MSE	NCC	SC	SC (Filter)	SC (Eroded)
Fish.jpg	1.3057	1	0.7626	0.7626	1.0855
Kat.jpg	1.4346	1	0.8060	0.8159	1.1877
Mario.jpg	1.0963	1	0.7652	0.7650	1.0914
Dog.jpg	1.4785	1	0.7637	0.7727	1.0968
Chick.jpg	1.3203	1	0.7526	0.7613	1.0860

TABLE .IX Observations for Recovered and Original cover image

Filenames	NCC	SC
Fish.jpg	1	1
Kat.jpg	0.9999	0.9999
Mario.jpg	1	1
Dog.jpg	1	1
Chick.jpg	1	0.9999

The above tables VI-IX show that the values are within standard measurements. For different images the values are in acceptable range. Even if watermark image is changed for a cover image the value remains same.

VI. CONCLUSION

The experiment is carried out on different images and images with varying size such as 204*204,256*256, 400*400 etc and different type of images like jpeg, tif, png etc. where the results are found to encouraging. It gives exact image back after extraction with NCC and Structural count value as 1. The image extracted is clear and has no distortion. The PSNR value obtained are all within the acceptable range. A scheme with the constant embedding capacity has been proposed where this embedding capacity is independent with the host signal. The limitations of vector quantization and transplantation attacks are addressed. A comparative analysis is carried out on different images and their types using graphs and tables showing how the proposed scheme works well on different parameters on spatial domain. To eliminate noise from image filters are used.

REFERENCES

[1] Image Watermarking in the Real World" Extended Abstract Adrian Perrig Andrew Willmott Computer Science Department Carnegie Mellon University March 9, 1998

[2] Digital Watermarking Scheme Exploiting Non-deterministic Dependence for Image Authentication Chang-Tsun Li and Yinyin Yuan Department of Computer Science. University of Warwick Coventry, CV4 7AL, UK

[3] U P. S. L. M. Barreto, H. Y. Kim, and V. Rijmen, "Toward secure public-key block wise Fragile authentication watermarking," in IEE Proceedings - Vision, Image and Signa Processing, vol. 148, no. 2, pp. 57 – 62, April 2002.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in Proc. Int.Conf. Image Proceesing, vol. II, pp. 157-160, Rochester, New York, USA, September, 2002.

[5] M. Goljan, J. J. Fridrich, and R. Du, "Distortion-free data embedding for images," Proceeding of the 4th Information Hiding Workshop, pp. 27-41, Pittsburgh, PA, USA, April 2001.

DOI 10.17148/IJARCCE.2015.4894

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

[6] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," US patent, 6 278 791, 2001.
[7] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in Proc. IEEE Intl. Conf. Image Processing, vol. I, pp. 501-504, Barcelona, Spain, September, 2003.
[8] J. J. Fridrich, M. Goljan, and N. Memom, "Cryptanalysis of the Yeung–Mintzer fragile Watermarking technique**,"** Journal of Electronic Imaging, vol. 11, no 2, pp. 262-274, April 2002.
[9] C.-T. Li, "Digital fragile watermarking scheme for authentication of JPEG images image Authenticity," IEE Proceedings – Vision, Image, and Signal Processing vol. 151, no. 6, pp. 460 – 466, December 2004.
[10] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent Invisible watermarking schemes," IEEE Trans. Image Processing, vol. 9, no. 3, pp. 432-441, March 2000.
[11] Watermark embedding and detection Shanghai Jiao tong University September 2006
[12] J. M. Barton, "Method and apparatus for embedding authentication information within digital data," U. S. Patent 5 646 997, 1997.
[13] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in Proc. EUSIPCO 2000, Tampere, Finland, September 2000.
[14] Dr. Dayanand.g.savakar and anand ghuli "digital watermarking-a combined approach by dwt, chirp-z and fast Walsh-hadamard transform", int.j.computer technology & applications,vol 5 (6),2006-2010.
[15] Chang-Tsun Li and Yinyin Yuan "Digital Watermarking Scheme Exploiting Non-deterministic Dependence for Image Authentication"
[16] Reversible watermarking scheme with image-independent embedding capacity. IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 6, December 2005
[17] AKRAM M. ZEKI et al. Steganographic Software: Analysis and Implementation IJCC Issue 1, Volume 6, 2012.
[18] C.-T. Li "Reversible watermarking scheme with image-independent embedding capacity C.-T." IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 6, December 2005

BIOGRAPHIES

Pooja Loni received B.E. degree in Computer Science Engineering from Visvesvaraya Technological University of Belgaum in 2013. Currently pursuing her M.Tech degree in Visvesvaraya Technological University of Belgaum. Her research interests include Image Processing and Wireless Sensor Networks.

Dr. Virendra. S. Malemath is currently a Head of Computer Science & Engg, KLE DR M S Seshagiri College of Engg. & Tech., Belgaum. He did his Bachelors in Engg, in Electronics & Communication Engg, from Karnataka University, Dharwad in the year 1993, did his MS in Software Systems from BITS Pilani Rajasthan in 1998 and received his PhD in Computer Science from Gulbarga University, Gulbarga, India in 2009. His research interests are document image processing medical and pattern recognition. He has published more than 60 articles in peer reviewed international journals and conferences.

Mrs. Sushma V Chaugule is working as Assistant Professor in the Department of Computer Science and Engineering in KLE Dr M S Seshagiri College of Engineering and Technology, Belgaum, Karnataka, India. She has obtained her BE in CSE in the year 2005 and M.Tech Digital Communication and Networking in the year 2007. Her areas of Research Interest are Image Processing and Pattern Recognition, Document Image Analysis and Medical Image processing. She has number of publications in peer reviewed International conferences

Anup Kalyanashetti received B.E. degree in Computer Science Engineering from Visvesvaraya Technological University of Belgaum in 2012. Currently pursuing M.Tech degree in Visvesvaraya Technological University of Belgaum. His research interests include Wireless Sensor Networks and image processing.