A HYBRID FRAGILE HIGH CAPACITY WATERMARKING TECHNIQUE WITH TEMPLATE MATCHING DETECTION SCHEME.

R.Prashanthi

Applied Electronics,
Government College of Technology,
Coimbatore, India.
E-mail: prashanthipaper@gmail.com

Abstract— With the rapid growth in the development of digital content, the terms security and privacy are very challenging issues. Watermarking is a broad interesting field which provides way in hiding an informal or formal data in another for maintaining intellectual property rights. The key perspectives of watermarking are security, robustness, invisibility and capacity. In the proposed technique the capacity is increased by embedding two RGB images in one RGB image. The invisibility of the hidden information is obtained by employing LSB substitution. The security is enhanced using a novel template matching detection scheme .The proposed fragile watermarking system destroys the watermarks when modified or tampered thus providing integrity and authentication features.

Keywords: Watermarking, Fragile, invisibility, security, robustness, capacity

I. INTRODUCTION

[1]Watermarking is descendent of a technique known as steganography which has been in existence for at least a few hundred years. In watermarking one or more information which can either be a text, image, audio or video is embedded in another to prevent forgery and unauthorized replication of digital content.

The various key perspectives of watermarking are described below. Imperceptibility: The embedded watermarks are imperceptible both perceptually as well as statistically and do not alter the aesthetics of the multimedia content that is watermarked. The watermarks do not create visible artifacts in still images, alter the bitrate of video or introduce audible frequencies in audio signals. Robustness: Depending on the application, the digital watermarking technique can support different levels of robustness against changes made to the watermarked content. If digital watermarking is used for ownership identification, then the watermark has to be robust against any modifications. On the other hand, if digital watermarking is used for content authentication, the watermarks should be fragile, i.e., the watermarks should get destroyed whenever the content is modified so that any modification to content can be detected. Inseparability: After the digital content is embedded with watermark, separating the content from the watermark to retrieve the original content is not possible. Security: The digital watermarking techniques prevent unauthorized users from detecting and modifying the watermark embedded in the cover signal. Capacity: Corresponds to the amount of information which can be carried in the image by the watermarking process.

[2]The watermarking techniques are classified into several types based on parameters. Based on the domain it is classified in to spatial and frequency domain watermarking system. Taking in to account the type of documentation it is classified in to text, image audio or video watermarking technique. It is classified in to two types based on perception of human sensory system: visible and invisible watermarking system. Invisible watermarking system is further of two type's robust and fragile watermarking technique. Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. As opposed to this, fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with. In this paper a completely fragile watermarking system is approached. [3]The various application of fragile watermarking are

- Ownership Assertion – to establish ownership of the content.
- Security in Telemedicine: to provide treatment from remote and this requires transfer of medical images confidentially and securely.
- Secured E-voting System: to prevent fraud and to protect voter's privacy.
- Fingerprinting – to avoid unauthorized duplication and distribution of publicly available multimedia content

- Authentication and integrity verification – the authenticator is inseparably bound to the content whereby the author has a unique key associated with the content and can verify integrity of that content by extracting the watermark
- Content labeling – bits embedded into the data that gives further information about the content such as a graphic image with time and place information
- Usage control – added to limit the number of copies created whereas the watermarks are modified by the hardware and at some point would not create any more copies (i.e. DVD)
- Content protection – content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed

The rest of the paper is organized as follows .Related work is briefly explained in Section II. The proposed watermark embedding technique with improved capacity and invisibility is explained in Section III. Section IV describes the highly secured template matching watermark detection scheme. Experimental results and discussion are presented in Section V. Section VI provides the conclusion of the work and presents the future work.

II. RELATED WORK

[4] and [5]Probably one of the simplest techniques used in the spatial domain is the LSB modification. This method encodes a signal in the least significant bits. The invisibility of the watermark is achieved on the assumption that the LSB data are visually insignificant. There are two ways of doing an LSB modification: Watermarking methods based on modifying the least significant bit(s) of a cover signal can be applied to every media type robust to bit modifications. Usually the LSB of a media (e.g. sample or pixel) can be changed without degrading the perceived quality. Additional gate functions can be applied to ensure a high transparency by allowing the usage of least significant bits only in those parts of the cover signal where the overall energy is high. This operation can be repeated for each sample or pixel, enabling a very high capacity. The watermark, however, was not robust to additive noise

[6]In this method four diversified pixel intensity matrices of the original and watermark image are created. Of the eight matrices created four diversified pixel matrices of the watermark are scales by one factor and the diversified pixel matrices of original image are scaled by another factor. These matrices are added to form the watermarked image. The value of the two factors is adjusted to change the visibility level.

[7]The color image is transformed in to luminance and chrominance form. The luminance part is taken for processing. The entire image is divided into 8X8 blocks. The log average of the whole image and the individual blocks are determined. The watermark is embedded in those blocks which have log average value greater than or equal to the log average value of the entire image. The image is then converted to the RGB format.

[8]Cynthia Palma Hernandez proposed a fragile watermarking technique for image authentication in mobiles. In this scheme, the watermark is generated by pseudo-random chaotic process that involves the values of the original image pixels, i.e., its image content dependent .The detection of the watermark is performed only with the information of the parameters used. If the image is not attacked the watermark embedded can easily be extracted.

Unlike, the above approaches where the maximum capacity is embedded an RGB image in another RGB image. This paper approaches a complete fragile watermarking technique which can embed two RGB images in one RGB image and a highly secure template matching watermark detection scheme

III. PROPOSED SYSTEM

The proposed watermarking technique produces a fragile watermarking system thereby helping in maintaining the trade-off between the various properties of watermarking.

The capacity which depicts the amount of information hidden in the cover image is first taken in to account. Previous works embed a RGB image in another RGB image which is the highest level of capacity .This is because the amount of information in a RGB image is three times higher than the amount of information in a gray scale image. In the proposed system two RGB images are embedded in a RGB image or six gray scale images are embedded in a RGB image. This is achieved by taking in to account the red, green and blue planes of an image. The former case is considered first. The two color watermark images are interleaved pixel wise using two base templates to form the final template which is the watermark image. The latter case where six gray scale image are considered and taken in to consideration. Two base color templates are created. The three planes of the template red, green and blue are used to impose three gray scale images. Thus six gray scale images are imposed in two base templates. The two base templates are further interleaved to form the final watermark image .Thus by this way the capacity which is one of the key properties is improved.

Next we take in to account the invisibility and robustness of the watermarking technique. The LSB of a pixel in a image contains less information about the image and changes to it does not alter the invisibility level of the image to the naked eye. Likewise the MSB of a pixel in a image contains the dominant information and changes to it alters the visibility level of the image. Thus we make use of this property to enhance the invisibility level of an image. The MSB of the pixels of the watermark image is embedded in to the LSB of the pixels of the host image. This therefore preserves the information in the watermark image together preventing it visibility in the host image.

Further to improve the security and robustness of the image that is transferred a fragile watermarking system can be employed in the proposed watermarking technique. The fragile watermarking system destroys the watermark if is attacked by an intruder. This is achieved by using a template matching scheme. In this approach the watermark is embedded in the host image in the above proposed method and a template of it is created and stored as a 2D key value in the database. In the extraction side the watermarked image is used to create a template and the 2D key value. A correlation matching of both the key values is performed, if it matches the watermark images are extracted and if does not match the, entire host image gets destroyed.

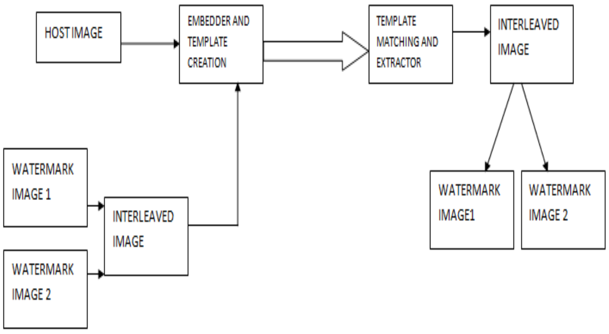

Figure 1. Block diagram of proposed watermarking system

A. Algorithm

1) The host image and two watermark images are all resized to same size.

   Host Image= H_{img}

   Watermark Images=W_{img1}&W_{img2}

2) The two color watermark images are imposed to two base templates Template=T1 & T2

   T1 (R:G:B) = W_{img1}(R:G:B)

   T1 (R:G:B) = W_{img1}(R:G:B)

3) The two templates are interleaved to form the watermark image. Arrange the pixels of templates alternatively in odd and even columns to form the interleaved watermark image.

4) The watermark image is then embedded to the host image by LSB substitution of pixels of watermark image to MSB substitutions of pixels of host image

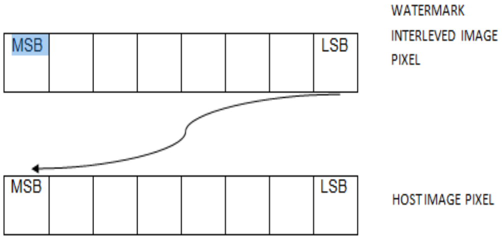

Figure 2. LSB substitution of one pixel.

5) A template is created for the watermarked image and 2D key value is obtained from the template.

IV. TEMPLATE MATCHING DETECTION SCHEME

The watermarked image is the input to the watermark detector. To create a fragile watermarking system a template of the watermarked image is created in a similar manner that is done above. A 2D key image value is obtained from the template. A correlation checking of the 2D key value is done. If it produces a correct result the watermarks are extracted. If it does not produce a correct result it implies that the watermarked image is been subjected to changes and it therefore destroys the watermark.

A. *Algorithm*

1) The input to the watermark extractor is the watermarked image. A template is created in a similar manner and a 2D key value is obtained.
2) A 2D correlation checking is done. If the watermarked image is not subjected to any changes , then checking yields to a positive results proving to be a fragile watermarking system.
3) Then the interleaved watermark image is first obtained by bitwise pixel comparison.
4) The watermark images are then obtained from the interleaved image by arranging odd and even pixels.
5) The images are further modified by padding of missing pixels relating it to the neighbor pixels.

V. RESULTS AND DISCUSSION

[9]In a fragile watermarking system the performance of the algorithm is tested in terms of three key perspectives

CAPACITY AND ROBUSTNESS: The amount of information hidden in the host image is taken in to account. The larger the capacity the more robust the algorithm is.

INVISIBILTY: This describes the inability of human naked eye to view the watermarks embedded in the host image.

SECURITY: The security is the way the watermarked image behaves to attacks (i.e) the watermarks should get destroyed when disturbed by an intruder or actions on it in fragile watermarking system.

Two cases are considered .In the former RGB host and RGB watermark images of same sizes are taken and experimentally analyzed. The host image is GCT building and is of size 512*512 shown in figure3.The watermark images are GCT logo and a text image and both are of size 512*512 and are shown in figure 4.

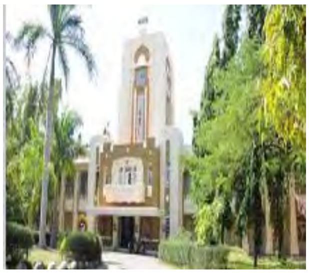

Figure 3. Host Image

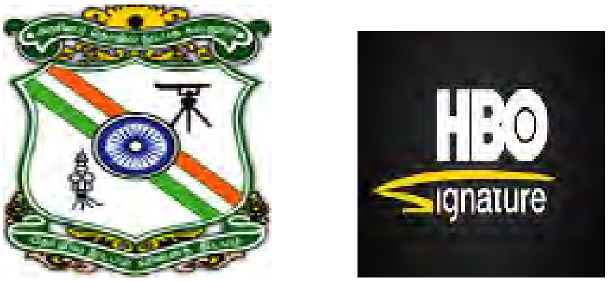

Figure 4. Watermark images (RGB)

The watermarking is performed using the above mentioned technique and the watermarked RGB image is shown in figure 5.

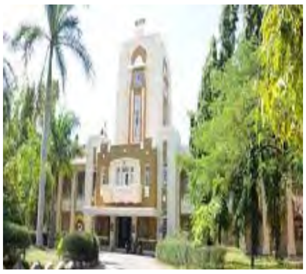

Figure 5. Watermarked Image.

The watermarked image obtained is used to create a template and is shown in figure 6

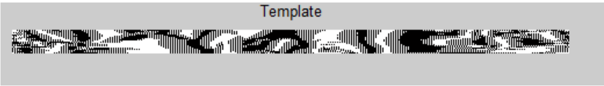

Figure 6. Template

In the detector if the watermarked image is not attacked or made changes the template will match and the watermark will be extracted. The extracted watermarks are shown in figure 7.

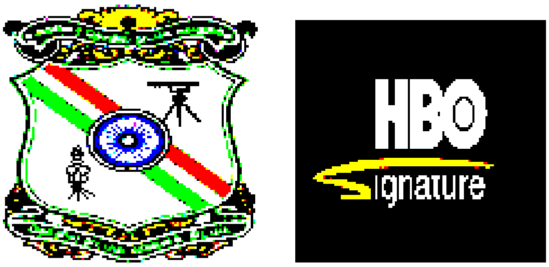

Figure 7. Extracted Watermark images

In the later case RGB host image and 6 gray scale watermark images all of size 512*512 are taken and is shown in figure 8 and 9..

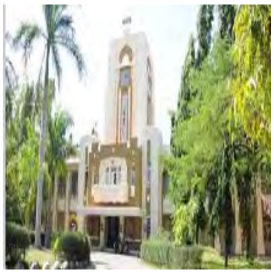

Figure 8. Host image

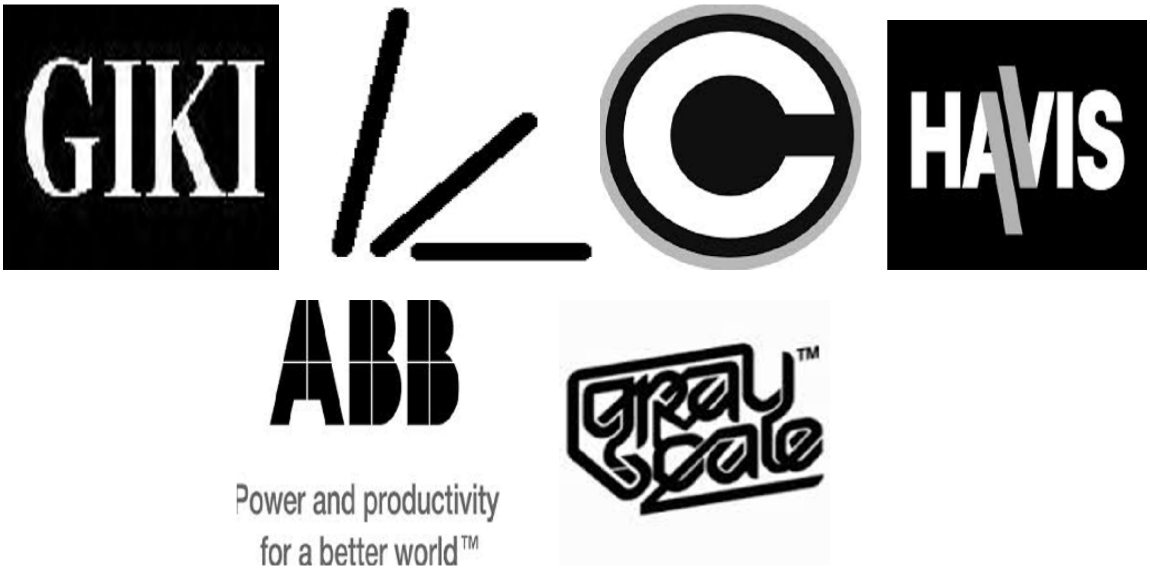

Figure 9. Watermark images (Gray scale)

The watermarking is done by interleaving two base templates. Red, green, blue planes are individually used to embed three gray scale images. Thus six gray scale images can be stored in two base templates. This is because a color image stores three times more information than a gray scale image. The invisible watermarked image is shown in figure 10.

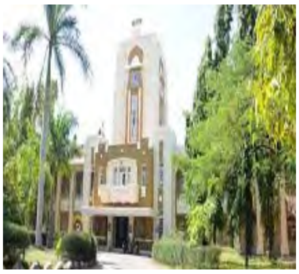

Figure 10. Watermarked image.

A template is created and sent to the detector where a template matching scheme is employed. If the result is success the watermarks are extracted. The extracted watermarks are shown in figure 11.

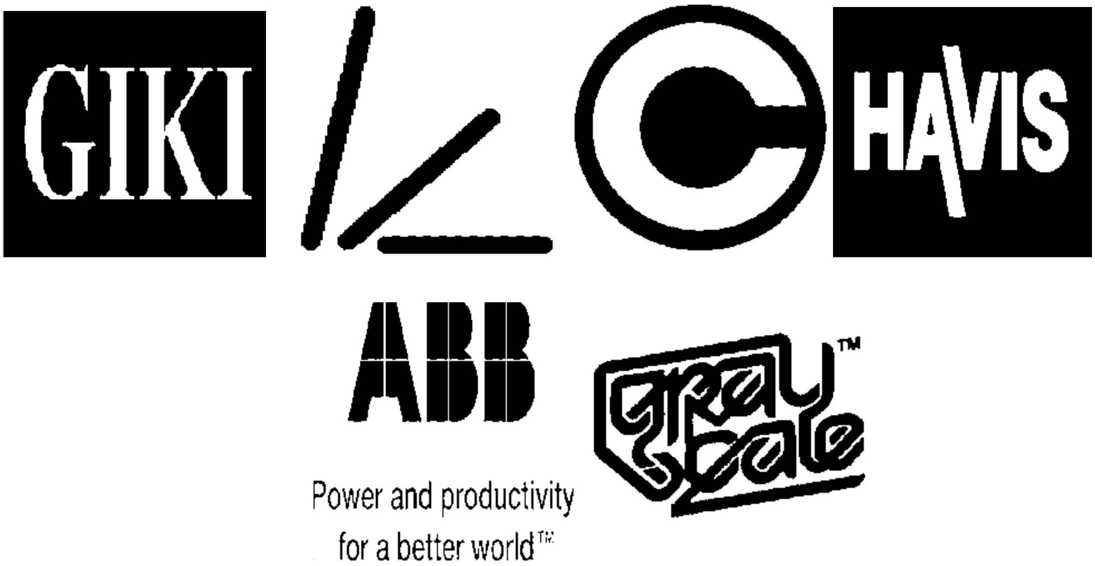

Figure 11. Extracted watermark images

The results are further analyzed in terms of peak signal to noise ratio and noise correlation. The perceptual quality of the host image after watermarking is determined by the peak signal to noise ratio.

TABLE I. PERFORMANCE ANALYSIS

TECHNIQUES	PSNR (dB)	INVISIBILITY LEVEL	CAPACITY IN TERMS OF WATERMARK
[7] Jamal.A	62.49	Low	1 gray scale image
[10]Patil (2011)	30.53	High	1 gray scale image
[8]Palma Hermandez (2011)	48.13	High	1 gray scale image
[11]U.M.Gokhale (2012)	50.44	Medium	1 gray scale image
[12]Dr.M.Mohammed (2012)	59.11	High	1 gray scale image
[13]S.K.Ghosal (2013)	39.64	High	1 RGB image
[14]Taha. Jassim (2013)	47.59	High	1 RGB image
Proposed Case1	53.23	High	2 RGB images
Proposed Case2	53.94	High	6 gray scale images

It is well seen from the table 1 that the proposed technique maintains the trade off between the key perspectives of watermarking. It increases the capacity, robustness and security of the system there by maintaining the invisibility level of the watermarked image.

VI. CONCLUSION AND FUTURE WORK

Thus the fragile watermarking scheme proposed in this paper has the ability to detect images that are attacked or made changes in the communication. This feature is enabled by embedding watermark which is of very high capacity in the proposed scheme and any changes to the watermarked image destroys the watermark indicating that is been intruded. The future work aims in using frequency domain techniques to further improve the robustness.

REFERENCES

[1] F. Cayre, C. Fontaine, and T. Furon, “Watermarking security: theory and practice,” IEEE Trans. on Sig. Proc., vol. 53, no. 10, pp. 3976–3987,Oct. 2005.

[2] Mr. Krunal and Mr .Lokesh,“Current classification and introduction of Watermarking Techniques in Digital Images,” International Journal of Engineering Research and Applications, Vol. 3, Issue 1,pp. 840-846, January –February 2013.

[3] Prabhishek Singh and R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks,” International Journal of Engineering and Innovative Technology, Vol.2, Issue 9, March 2013.

[4] Kekre,DhirendraMishra,“Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB’s Method for Images,” International Journal of Computer Applications ,Vol. 45,No.1, May 2012

[5] Puneet Kr SharmaS and Rajni, “Analysis of image watermarking using least significant bit algorithm,” International Journal of Information Sciences and Techniques, Vol.2, No.4, July 2012

[6] Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar andVenkat Krishnan Balasubramanian, “Performance Comparison of Novel, Robust Spatial Domain Digital ImageWatermarking with the Conventional Frequency Domain Watermarking Techniques,”International Conference on Signal Acquisition and Processing,2010.

[7] Jamal A. Hussein, “Spatial Domain Watermarking Scheme for Colored Images Based on Log-average Luminance,”Journal of computing , Vol.2,Isuue1,January2010.

[8] Cynthia Palma Hernandez and Cesar Torres-Huitzil ,“A fragile watermarking scheme for image authentication in mobile devices,” Electrical Engineering Computing Science and Automatic Control International Conference ,2011.

[9] Wei-Chin Ku & Te-Chih Chou and Hsin-Lung Wu & Jen-Chun Chang, “A fragile watermarking scheme for Image Authentication with Tamper Detection and Localization,” Fourth International Conference on Genetic and Evolutionary Computing,2010.

[10] Prasad and Shefali Sonavane,“FragileWatermarking Scheme for Image Tamper Detection,” International Conference on Communication Systems and Network Technologies,2011.

[11] U. M. Gokhale and Y.V.Joshi, “A Semi Fragile Watermarking Algorithm Based on SVD-IWT for Image Authentication,” International Journal of Advanced Research in Computer and Communication Engineering,Vol. 1, Issue 4, June 2012.

[12] Dr.M.Mohamed Sathik and S.S.Sujatha,“Authentication of Digital Images by using a semi-Fragile Watermarking Technique,” International Journal of Advanced Research in Computer Science and Software Engineering,Vol.2, Issue 11, November 2012.

[13] S.K.Ghosal and J.K. Mandal, “ A fragile watermarking based on legendre transform for color images,” An International Journal (SIPIJ) Vol.4, No.4, August 2013.

[14] Taha. Jassim and Raed Abd-Alhameed, “New Robust and Fragile Watermarking Scheme for Colour Images Captured by Mobile Phone Cameras,”15th International Conference on Computer Modelling and Simulation,2013.

[15] Rafael C.Gonzalez, Richard E. Woods, Steven L. Eddin, “Digital Image Processing Using MATLAB”. Electronics Industry Publishing House. 2006.