Secured Semi-Fragile Watermarking for Color Images Against Geometric Attacks

R. Nithya Devi[1], C. Kavitha[2]
[1]*M.E (CSE),* [2]*AP (Sl.G-1)/CSE*
[1,2]*Erode Sengunthar Engineering College*

Abstract - The watermarking process is performing arts of hiding a message related to a digital signal (i.e. an audio, video and image) within the signal itself. Watermarking applications are copyright control, broadcast monitoring and device control. The image authentications are classified into two types. They are signature-based and fragile watermarking schemes. Signature-based schemes are the host image which is applied to the hash function and hashed result is encoded using a public key cryptosystem to produce the output signature. The fragile-based scheme present watermark bits which are embedded into the host image in order to check the integrity and authenticity without the need to store additional data. The projected scheme is present a secure Semi-Fragile Watermarking for color images against geometric attacks. The color image transformation is done to HSV color space, suiting to the corresponding color band. Each color band channel is divided into 4×4 non-overlapping blocks and each 2×2 sub block is selected. The actions for color image watermarking are embedding, verification and recovery. The semi-fragile watermark distribution is done with a private key to have a secure mapping of blocks. This method handled subjective and objective Perceptron for watermark images and geometric attacks. The performance measure of proposed semi fragile watermarking on color images are done with following metrics are watermark image size, original image size, geometric transformation rate, PSNR of watermarked images and average mean square error rate.

Key Terms: Semi-Fragile Watermark, Color Image Watermark, Geometric Attacks.

I. INTRODUCTION

Image processing is a technical method handles to translate an image into digital form and executed in various processes, in order to obtain an improved image or to take some valuable information from the image processing. Digital Watermarking is a technique of protecting the digital media in embedding extra information called digital signature or watermark into the digital substances such that it can be discovered, extracted later to make an assertion about the multimedia data. A watermark is automated an arbitrary signal, a significant message logo that can be used for ownership secure, copy control and authentication. In regulate to watermarking as a method of exclusive rights secure, high level of strength and decrease the visibility should be guaranteed, and single authorized users should expand access to the watermark data. Semi-fragile watermark fragile to malicious alterations while forceful to incidental exploitations is drawing one or more attentions in image authentication. Selective authentication utilizes the methods based on semi fragile watermarking or image content signatures to produce few type of strength against particular and desired exploitations.

II. PROTECTION OF SEMI-FRAGILE WATERMARKING FOR COLOR IMAGES AGAINST GEOMETRIC ATTACKS

In this work plan a secured semi-fragile watermarking technique for colored images against geometric attacks. This method is mostly handled for copy right security in which the objective of watermark is to maintain low level all types of issues that mean to avoid the watermark while securing the perceptual worth of the original media.

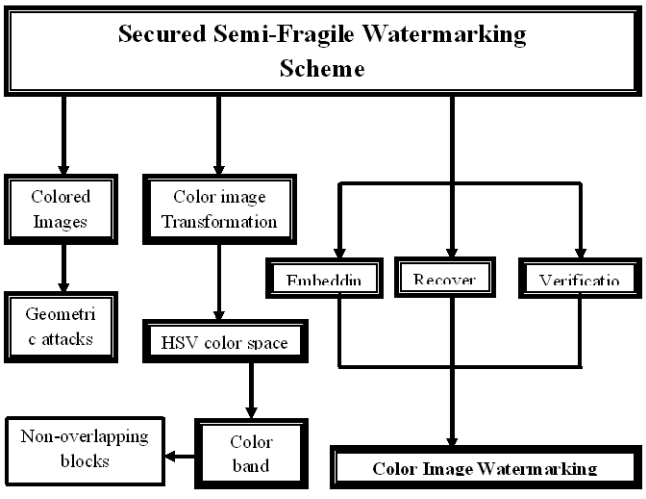

Fig: 2.1. Architecture Diagram of Protection of semi-fragile watermarking scheme

This method improves the subjective and objective perception of the watermarked images. Secure of semi-fragile watermarking procedure are embedding, verification and recovery. The final is used for data authentication and is perceptive to any type of processing that may transpire. A fragile watermark is especially perceptive and planned to discover all possible change in a marked image, but in most multimedia applications, minor data modifications are suitable as long as the content is authentic. A semi-fragile watermark is forceful to suitable content protecting managements such as lossy compression while fragile to malicious distortions such as content alteration.

The protection of semi-fragile watermarking scheme is divided into three phases are:

a) Color Image Watermarking

b) Embedding and Verification

c) Recovery against Geometric Attacks

a) Color Image Watermarking

To determine the security issues of color image, an efficient, robust and invisible color image watermarking method. This method embeds the watermark from cover image in (Red, Green, Blue) RGB space. The key color image in RGB color space is transformed to HSV color space.

The Color image watermark generation process is

- Selecting all channels
- Divide the image into non-overlapping blocks
- Set two LSBs of its each sub block to zero
- Compute the average intensity mean of block and sub-block
- Encode it six to eight binary bits.

Once embedding process is done for concatenate all the channels and transform the images from HSV domain to RGB by taking inverse transform to obtain watermarked image.

b) Embedding and Verification

The embedding space is created by setting two LSBs of chosen sub-block to zero, which hold the authentication and recovery information. Select the channel of image is divide into non overlapping 4×4 blocks perform a secure mapping of blocks with a private key. Embed watermark into each mapped 4×4 block's and 2×2 sub-block two LSBs of HSV channel. For verification of semi-fragile watermark identification parity bits are computed for each 2×2 sub-block. Watermark color image is transformed from RGB to HSV color. Select the channel divide its 2×2 sub-blocks to extract the authentication and parity bits from designated LSBs. After extraction of desired bits from channel, set the two LSBs to zero. Compare the process of extracted and generated parity bits, if they found same tested image is authentic otherwise tampered.

c*) Recovery against Geometric Attacks*

This method provides robust and geometric invariant watermarking scheme using block histogram and intensity-level histograms. For recovery process is intensity mean of each 2×2 sub-block is computed and encoded up to six to eight bits depending upon color band channel selection. For forged image identify those blocks that are tempered by setting their pixels value to zero. Size of sub-block is suitable for correct localization of color components in watermarked image and fast computation resist against geometric attacks. In case of HSV channel assign the earlier computed intensity mean in verification phase to the tampered block of each pixel. The target block hold the source block information is determined by executing 2D-Torus automorphism using a private key to have secure mapping of blocks. The perceptibility of watermarked image is high and PSNR value for all the tested images is greater than 42 db. The recovery against geometric attack is correctly localizes the tampering with full recovery of the original work.

III. PERFORMANCE METRICS

In this section evaluate the performance of secured semi-fragile watermarking is done for color images against geometric attacks through Matlab environment. One of the major contributions of this work is protecting semi-fragile watermarking for colored images and geometric attacks. The performance metrics of the parameters is watermark image size, original image size, geometric transformation rate, PSNR of watermarked images and average mean square error rate.

The performance metrics are

- Geometric transformation rate
- PSNR of Watermarked Images

- Average Mean Square Error Rate

3.1. Geometric transformation rate

It is view that evaluation with the rate of geometric transformation can be effectively working in interframe codes to compensate problem. Dissimilar the conventional evaluation method that simply compensates translational motion, the transformation process facilitates very precise matching of non-uniform changes between images. But, high level sequences of images cannot be encoded among vectors alone. Although the fractional pixel accuracy of the geometric transforms compensation few errors do accumulate.

Table: 3.1. Watermark Image Size Vs Geometric Transformation Rate (%)

Watermark Image Size	Geometric Transformation Rate (%)	
	GIAT (Existing)	SSFW (Proposed)
10	60	79
20	58	77
30	55	76
40	53	73
50	50	71

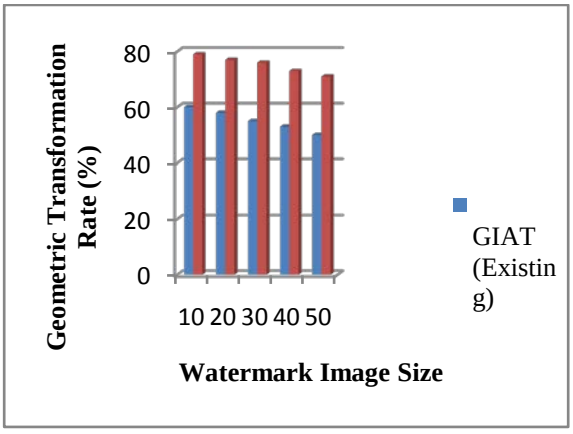

Fig: 3.1. Watermark Image Size Vs Geometric Transformation Rate (%)

Figure: 3.1 Demonstrate the rate of Geometric Transformation. X axis represents the watermark image size whereas Y axis denotes the Geometric transformation rate using both the Grayscale Image Authentication and Tamper detection (GIAT) Technique and our proposed Secured Semi-Fragile Watermark (SSFW) Technique. When the watermark image size increased, geometric transformation rate gets increases accordingly. The rate of geometric transformation is illustrated using the existing GIAT and proposed SSFW Technique. Figure 3.1.shows better performance of Proposed SSFW method in terms of image size than existing GIAT and proposed SSFW. The Secured Semi-Fragile Watermark (SSFW) Technique achieves 15 to 25% high performance of geometric transformation rate variation when compared with existing system.

3.2. PSNR of Watermarked Images

The value metric is based on PSNR. One commonly used measure to estimate the imperceptibility of the watermarked image is the peak signal to noise ratio (PSNR). The reality that the interpolation process is analyzed for all resample pixel, the multiplication operations build up to be an exclusive computation. Thus, the number of multiplication operations has to be kept to a minimum.

Table: 3.2. Watermark Image Size Vs PSNR of Watermarked Images (%)

Watermark Image Size	PSNR of Watermarked Images (%)	
	GIAT (Existing)	SSFW (Proposed)
10	48	36
20	56	45
30	67	54
40	79	68
50	84	71

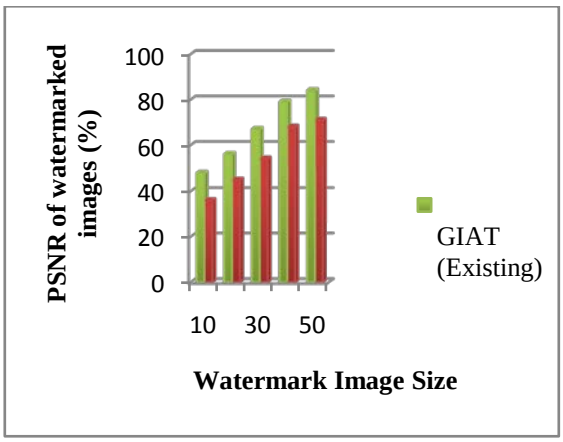

Figure: 3.2. Watermark Image Size Vs PSNR of Watermarked Images (%)

Figure: 3.2. Demonstrate the PSNR of watermarked images. X axis represents the watermark image size whereas Y axis denotes the PSNR of watermarked images using both the Grayscale Image Authentication and Tamper detection (GIAT) Technique and proposed Secured Semi-Fragile Watermark (SSFW) Technique. When the watermark image size increased, PSNR of watermarked images gets decreases consequently. The PSNR of watermarked images is illustrated using the existing GIAT and proposed SSFW Technique. Figure 3.1.shows better performance of Proposed SSFW method in terms of image size than existing GIAT and proposed SSFW. The Secured Semi-Fragile Watermark (SSFW) Technique achieves 10 to 15% high performance of PSNR of watermarked images variation when compared with existing system.

3.3. Average Mean Square Error Rate

They are subjective evaluation and objective valuation, respectively. Both of them obey the following assumption: In the holder of incidental attack, most of the watermark error pixels are isolated on the difference image or the extracted watermark.

Table: 3.3. Watermark Image Size Vs Average Mean Square Error Rate (%)

Watermark Image Size	Average Mean Square Error Rate (%)	
	GIAT (Existing)	SSFW (Proposed)
10	45	40
20	49	45
30	53	50
40	58	53
50	61	59

Figure: 3.3. Demonstrate the average mean square error rate. X axis represents the watermark image size whereas Y axis denotes the Average Mean Square Error rate using both the Grayscale Image Authentication and Tamper detection (GIAT) Technique and proposed Secured Semi-Fragile Watermark (SSFW) Technique. When the watermark image size increased, average mean square error rate gets decreases accordingly. The rate of mean square is illustrated using the existing GIAT and proposed SSFW Technique. Figure 4.3.shows better performance of Proposed SSFW method in terms of image size than existing GIAT and proposed SSFW. The Secured Semi-Fragile Watermark (SSFW) Technique achieves 5 to 10% high performance of rate of mean square error variation when compared with existing system.

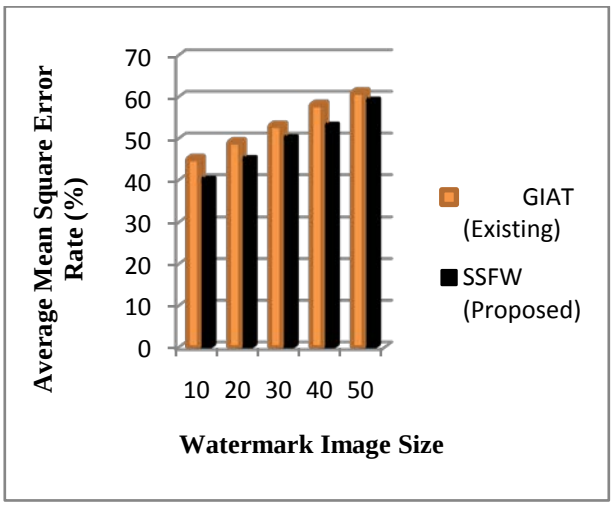

Figure: 3.3. Watermark Image Size Vs Average Mean Square Error Rate (%)

IV. CONCLUSION

This paper proposes a robust and geometric attack watermarking scheme using block histogram and intensity-level histograms. The give color image is first transformed from RGB color space capable for watermarking based applications. Authentication and parity bits are computed for each sub-block. The performance of planned semi fragile watermarking on color images are done with following metrics through the Matlab environment. In future work to extend the process of watermark embedding and extraction process will be improved and upgraded.

REFERENCES

[1] Xiaoyun Wu, Junquan Hu, Zhixiong Gu and Jiwu Huang, “A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters”, School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, 510275, P. R. China.

[2] Ching-Yung Lin and Shih-Fu Chang, “Semi-Fragile Watermarking for Authenticating JPEG Visual Content”, Department of Electrical Engineering, Columbia University, New York, NY 10027, USA.

[3] 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.

[4] Lintao LV, Hua fan, Jinfng Wang and Yuxiang Yang, "A Semi-Fragile Watermarking Scheme for Image Tamper Localization and Recovery", Journal of Theoretical and Applied Information Technology, 31 August 2012. Vol 42, No.2.

[5] Xiaojun Qi and Xing Xin, "A quantization-based semi-fragile watermarking scheme for image content authentication", Department of Computer Science, Utah State University, Logan, UT 84322-4205, United States

[6] Ghazali Bin Sulong , Harith Hasan(Corresponding author) , Ali Selamat , Mohammed Ibrahim and Saparudin, "A New Color Image Watermarking Technique Using Hybrid Domain", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012.

[7] P.Ramana Reddy, Munaga .V.N.K.Prasad and D. Sreenivasa RAO, "Robust Digital Watermarking of Color Images under Noise attacks", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[8] Baisa L. Gunjal and Suresh N.Mali, "Secured Color Image Watermarking Technique in DWT-DCT Domain", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.3, August 2011

[9] Ibrahim Alsonosi Nasir and Ahmed b. Abdurrman, "A Robust Color Image Watermarking Scheme Based on Image Normalization", Proceedings of the World Congress on Engineering 2013 Vol III, WCE 2013, July 3 - 5, 2013, London, U.K.

[10] Bum-Soo Kim, Jae-Gark Choi, Chul-Hyun Park, Jong-Un Won, Dong-Min Kwak, Sang-Keun Oh, Chang-Rim Koh and Kil-Houm Park, "Robust digital image watermarking method against geometrical attacks", Real-Time Imaging 9 (2003) 139–149.

[11] Dr.J.Veerappan and G. Pitchammal, "Geometric Attack Resistant Multilayer Image Watermarking Scheme for Providing High Security".

[12] V. Solachidis, S. Tsekeridou, S. Nikolopoulos and I. Pitas, "Self-Similar watermarks for counterfeiting geometrical attacks", Greece.

[13] Patrick Cousot and Radhia Cousot, "Verification of Embedded Software: Problems and Perspectives", 75230 Paris cedex 05, France.

[14] Akshya Kumar Gupta and Mehul S Raval,"A robust and secure watermarking scheme based on singular values replacement", *Sadhana* Vol. 37, Part 4, August 2012, pp. 425–440.

[15] Yan XING, Jieqing TAN, "A Color Image Watermarking Scheme Resistant against Geometrical Attacks", Radio Engineering, Vol. 19, No. 1, April 2010.