Robust & Secure Digital Image Watermarking Technique using Concatenation Process

Kamal Kant Hiran
Sr. Lecturer, Dept. of Information Technology,
Sikkim Manipal University, Ghana,
kamalhiran@gmail.com

Ruchi Doshi
Lecturer, School of Technology,
BlueCrest College, Ghana
doshiruchi18@gmail.com

***ABSTRACT**: In this paper, a secure digital image watermarking Algorithm is proposed to protect the digital images from illegal copying; based on this; quality will be managed by PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error). In the field of digital image processing digital piracy is the important phenomenon. With the exponential growth of internet and high speed networks operating throughout the world it is a challenging task to protect copyright of an individual creation. Digital image watermarking provides a feasible solution to protect copyright and authenticate the ownership of an intellectual property. The operation of embedding and extraction of the watermark is done in the frequency domain and spatial domain thereby providing robustness against common frequency-based attacks including image compression and filtering techniques.*

Keywords: Digital Image Watermarking, Image Processing, Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE).

I. INTRODUCTION

Information hiding can be mainly divided into three processes - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it**.** Stenography [11] is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker.

Watermarking is closely related to stenography [10] but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection [8] and owner authentication.

Digital image watermarking is divided into two types:

- Spatial Domain Image Watermarking
- Transform Domain Image Watermarking

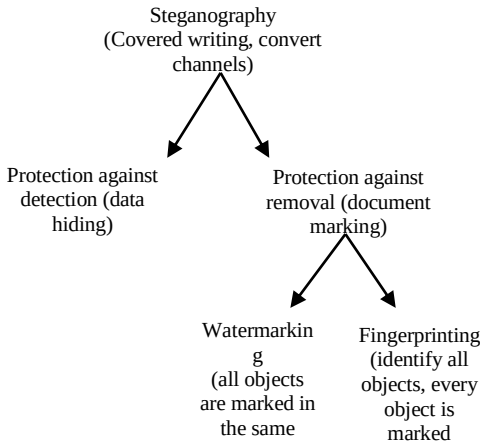

Figure 1. Watermarking block diagram.

In Spatial domain watermarking system [7] directly alters the main data elements, like pixels in an image to hide the watermark data. While in transform domain watermarking system [6] alters the frequency transform of data elements to hide the watermark data.

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. If a modification is done, this is called an attack. There are many possible attacks [4]. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy.

The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried by the signal itself.

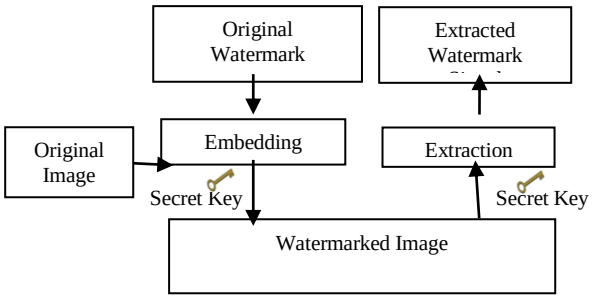

Figure 2. Watermarking Block Diagram.

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark onto the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark [12].

A. CLASSIFICATION OF WATERMARKING

- **Visible Watermarking:** The watermark is visible which can be a text or a logo used to identify the owner. Any text or logo to verify or hide content.

$$Fw = (1-\alpha)\, F + \alpha * W \qquad (1)$$

Where, Fw = Watermarked Image, α =constant; 0<=α<=1, IF α=0 No watermark, if α=1 watermark present F =original image, W =watermark.

- **Invisible Watermarking:** The watermark is embedded into the image in such a way that it cannot be perceived by the human eye. It is used to protect the image authentication and prevent it from being copied.

Invisible watermark can be further divided into three types:

- Robust Watermark: Invisible watermark cannot be manipulated without disturbing the host signal. This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark [7] should be such that it is invariant to various such attacks. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.
- Fragile Watermark: They are designed with very low robustness. They are used to check the integrity of objects.
- Public and Private Watermark: They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark [9] and if the original image is known it is called a non-blind watermark or a private watermark.

B. APPLICATIONS OF WATERMARKING

A popular application of watermarking techniques is to provide a proof of ownership of digital data by embedding copyright statements into video or image digital products.

- Automatic monitoring and tracking of copy-write material on WEB [13]. (For example, a robot searches the Web for marked material and thereby identifies potential illegal issues.)
- Automatic audit of radio transmissions: (A robot can "listen" to a radio station and look for marks, which indicate that a particular piece of music, or advertisement, has been broadcast) [11].
- Data Augmentation - to add information for the benefit of the public.
- Fingerprinting Applications [3] (in order to distinguish distributed data).

All kinds of data can be watermarked: audio, images, video, formatted text, 3D models, and model animation parameters.

II. RESEARCH METHODOLOGY

The proposed algorithm has been tested on various images. The figure shows the basic scheme of the watermarks embedding systems.

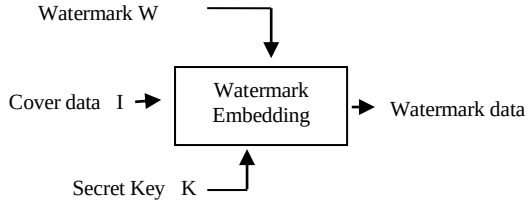

Figure 3. Watermarked Embedding System.

Inputs to the scheme are the watermark, the cover data and an optional public or secret key. The outputs are watermarked data. The key is used to enforce security. The figure shows the basic scheme for watermark recovery schemes.

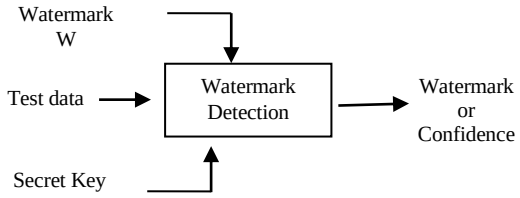

Figure 4. Watermarked Detection System.

Inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and/or the original watermark. The output is the recovered watermarked W or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

Step 1: Start

Step 2: A base image is taken in which the watermark will be added.

Step 3: The watermark image is taken, which will be added to the base image.

Step 4: Now both base and watermark image will be concatenated to get a watermarked image.

Step 5: Watermarked image will contain both base and watermark image.

Step 6: After this random noise is added.

Step 7: Noise is extracted.

Step 8: Then both the base and watermark image is extracted from watermarked image.

Step 9: Stop

Flow chart

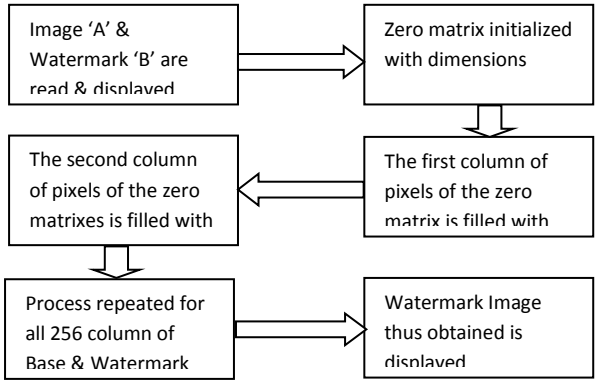

Figure 5. Concatenated Visible Watermarking block diagram

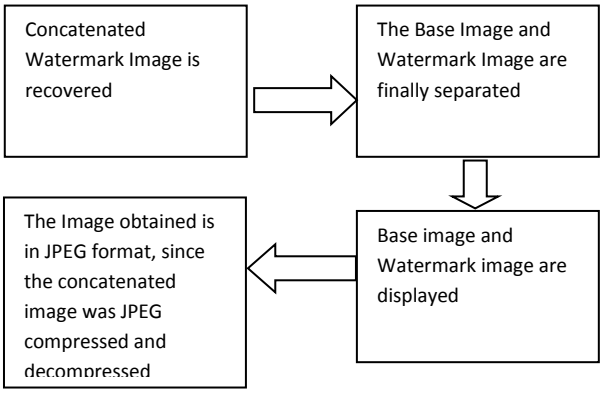

Figure 6. Recovery of base and Watermark

III. EXPERIMENT RESULTS AND ANALYSIS

- **Computing Peak Single to Noise Ratio (PSNR)**

PSNR is a measure of the peak error. When PSNR is higher than 30, the recomposed image has a very good quality and the eye could hardly tell the difference between the original and the recomposed image. This ratio is often used as a quality measurement between the original and a recomposed image.

The smaller the PSNR value is, the larger the difference between images will be. The larger PSNR value [2] implies the better image restoration. Usually, when the PSNR value is above 28dB, the image will have a better quality of recovery.

Calculating PSNR using following formula:

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right)db \qquad (2)$$

The mean square error (MSE) of two images of N x N pixels is defined as:

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(p_{ij} - p'_{ij}\right)^2 \qquad (3)$$

Where p_{ij} is the original cover image value and p'_{ij} is the embedded image pixel value. The higher the

pixel value the better the quality of the reconstructed image.

- **Mean Absolute Error (MAE)**

This is used to measure the average magnitude of the errors in a set of forecasts, without considering their direction. It measures accuracy of continuous variables. The mean absolute error is given by

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|f_i - y_i| = \frac{1}{n}\sum_{i=1}^{n}|e_i| \qquad (4)$$

As the name suggests, the mean absolute error is an average of the absolute errors

$$e_i = |f_i - y_i| \qquad (5)$$

Where, fi is the prediction and y_i is the true value.

Table 1: Different Images and their PSNR values

Input Image	PSNR (db)	MSE (db)	RMSE (db)	MAE (db)
Image I	37.771	114.570	10.703	17.202
Image II	37.781	261.625	16.481	25.620
Image III	38.751	271.655	15.452	27.670

If we change the watermark image and then concatenate with the original image then output can be seen as shown below. Here a colored watermark is taken. We can observe when this watermark is extracted from the watermarked image then its color changes.

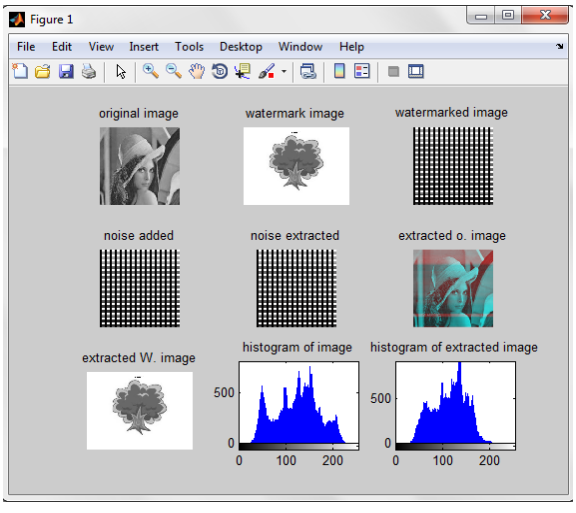

Figure 7. Simulation Result - 2

If we change the watermark image and then concatenate with the original image then output can be seen as shown below. Here a colored watermark is taken. We can observe when this watermark is extracted from the watermarked image then its color changes.

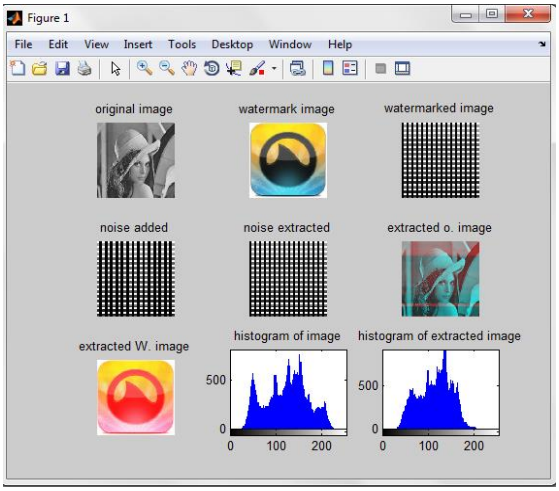

Figure 8. Simulation Result -1

IV. CONCLUSION

In the paper, a digital image watermarking algorithm is proposed. The algorithm presents a new method which is simple and effective. It provides a high level security for copyright protection by improving both the PSNR values. Thus, using MAT Lab, visible watermarking techniques are implemented. Noise is added to the images as a form of attack. The noise is later removed and the base and watermark images are separated from the watermarked image. Finally, a benchmarking of original and recovered image is done based on PSNR, MSE, RMSE and MAE. Simulation results indicate that the proposed algorithm is robust to common image-processing operations and some geometric attacks.

V. FUTURE WORK

In future research work, it is proposed to implement the watermark embedding & the extraction process in time and frequency domain using DCT, DWT and DFFT in order to improve the performance for different types of images specially color images as well as to make the proposed digital image watermarking scheme more robust and secure against various attacks.

VI. REFERENCES

[1] Deepak S. Turaga, Yingwei Chen, Jorge Caviedes (2004) "No reference PSNR estimation for compressed pictures" Signal Processing Image Communication, 2004, pp 173-184

[2] Hongwei Lu, Baoping Wan (2006) "Information Hiding Algorithm Using BMP Image", Journal of Wuhan University of Technology, Vol.28 (6), 2006, pp. 96-98, Doi: cnki:ISSN:1671-4431.0.2006-06-027

[3] Jian-quan Xie, Chun-Hua Yang (2007) "Adaptive hiding method of large capacity information", Journal of computer applications, vol. 27 (5), 2007, pp. 1035-1037, doi: CNKI:ISSN:1001-9081.0.2007-05-001

[4] Jianwei Zhang, Xinxin Fang, Junhong Yan (2006) "Implement Of Digital Image Watermarking LSB", Control & Automation, vol. 22(10), 2006, pp. 228-229, doi: cnki:ISSN:1008-0570.0.2006-10-083

[5] Juan Zhou, Shijie Jia (2007) "Design and Implementation of Image Hiding System Based on LSB", Computer Technology and Development, vol. 17 (05), 2007, pp. 114-116, doi: cnki: ISSN: 1673-629X.0.2007-05-034

[6] M. Jacome and G. de. Veciana (2000) "Design challenges for new application specific processors", IEEE Design and Test of Computers

[7] M. L. Miller, I. J. Cox, and J. A. Bloom (2001) "Informed embedding: exploiting image, Digital watermarking, Morgan Kaufmann Publishers Inc., San Francisco, CA

[8] M. N. Nobi and M. A. Yousuf (2011) "A New Method to Remove Noise in Magnetic Resonance and Ultrasound images" JOURNAL OF SCIENTIFIC RESEARCH, 2011, pp 81-89

[9] P. Geum-Dal,; Y. Eun-Jun, Y. Kee-Young (2008) "A New Copyright Protection Scheme with Visual Cryptography", Second International Conference on Future Generation Communication and Networking Symposia. pp. 60-63

[10] Qian-Lan Deng Jia-Jun Lin (2006) "A Steganalysis of LSB based on Statistics", Modern Computer, No.1, 2006, pp. 46-48, doi: cnki:ISSN:1007-1423.0.2006-01-010

[11] S. Gravano (2001) Introduction to Error Control Codes, Oxford University Press, USA

[12] Wei-Qi, J. Duo,M. S. Kankanhalli (2004) "Visual Cryptography for Print and Scan Applications". International Symposium on Circuits and Systems. pp- 572-575