Comparison between Naive Encryption & Pixel correlation method for optimizing the performance of Image Encryption by digital Watermarking

Megha Jyoti[1], Varinder Singh[2]
[1] jyoti5337@gmail.com, [2]singhgamer@gmail.com

ABSTRACT : *The recent advent in the field of multimedia proposed a many facilities in transport, transmission and manipulation of data. Along with this advancement of facilities there are larger threats in authentication of data, its licensed use and protection against illegal use of data. Digital watermarking is one of the most recent proposed systems to observe the authentication of licensed user over e-commerce applications and finds its uses in illegal applications like copying the multimedia data e.g. images, audio, video. The watermark indicates that data is containing copyright or not. To propose a measure against the illegal use of the images different available watermarking standards are studied. Then by taking the human visual system into consideration an algorithm is designed and it is implemented with use of C#. The algorithm designed is based on available watermarking methods but different in sense that it tends to prevent the illegal use of multimedia image. If any effort is done to copy or download the image in any unauthentic way i.e. without availability of any license or the Private Key issued by the owner the designed software damages the content of that image file so that the image looses its commercial value. This paper conducts a literature survey of watermarks used for images on Remote Web Server. It describes the previous work done on digital watermarks, including the analysis of various watermarking schemes and their results. Potential applications are discussed, and an implementation plan of the project is presented.*

Key Words: *Digital Watermarking, Copyright Protection, authentication, RGB.*

1. INTRODUCTION

Digital watermarking includes a number of techniques that are used to imperceptibly convey information by embedding it into the cover data [6]. There has always been a problem in establishing the identity of the owner of an object. In case of a dispute, identity was established by either printing the name or logo on the objects. But in the modern era where things have been patented or the rights are reserved (copyrighted), more modern techniques to establish the identity and leave it in tampered have come into Picture. Unlike printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data [7]. Watermarking, as opposed to steganography, has an additional requirement of robustness against possible attacks. An ideal steganographic system would embed a large amount of information perfectly securely, with no visible degradation to the cover object. An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. Over the past few years, there has been tremendous growth in computer networks and more specifically, the World Wide Web. This phenomenon, coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security; images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this tough issue. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image. This paper is a literature survey of digital watermarks. Its objective is to summarize the previous work done on digital watermarks and to detail the implementation plan of the project. The paper is organized as follows: Section 2 gives a general description of a digital watermark. Section 3 describes selective encryption for uncompressed images Section 4 explains the potential applications of watermarking, and section 5 presents the implementation plans for the project. Finally, section 6 gives a conclusion of the work done.

2. THE DIGITAL WATERMARK-A BRIEF DESCRIPTION

As a side effect of these different requirements, a watermarking system will often trade Capacity and perhaps even some security for additional robustness [9].The working principle of the watermarking techniques is similar to the steganography methods. A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a *key* which could be either a public or a secret

key. The *key* is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in Figures

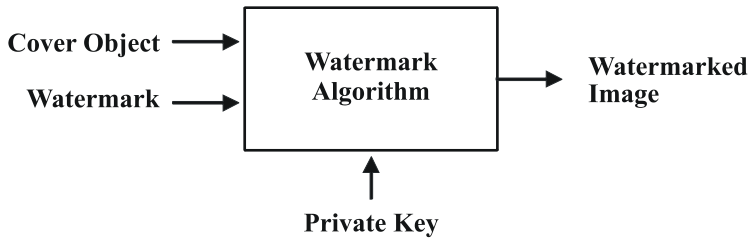

Fig 2.1 : *General Watermarking Block Diagram*

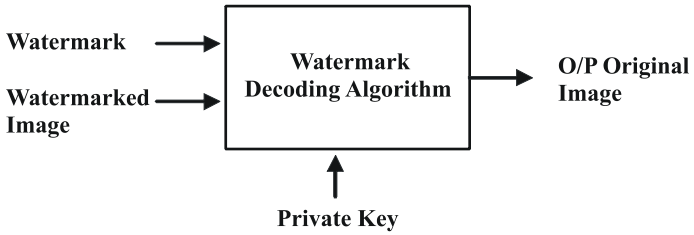

Fig 2.2 : *General Watermarking Decoding to recover Original Image*

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data *W.* The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark

W. In general, watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Ideal properties of a digital watermark have been stated in many articles and papers [1-3]. These properties include:

1) A digital watermark should be perceptually invisible to prevent obstruction of the original image.
2) A digital watermark should be statistically invisible so it cannot be detected or erased.
3) Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation.

4) Watermark detection should be accurate. False positives, the detection of a no marked image, and false negatives, the non-detection of a marked image, should be few.

5) Numerous watermarks can be produced. Otherwise, only a limited number of images may be marked.

6) Watermarks should be robust to filtering, additive noise, compression, and other forms of image manipulation.

3. SELECTIVE ENCRYPTION OF UNCOMPRESSED IMAGES

A very effective method to encrypt an image, which applies to a binary image, consists in mixing image data and a message (the key in some sense) that has the same size as the image: a XOR function is sufficient when the message is only used once. A generalization to gray level images is straightforward: encrypt each bitplane separately and reconstruct a gray level image. With this approach no distinction between bitplanes is introduced although the subjective relevance of each bitplane is not equal. [12]

3.1 Description of a "naive" method

Figure shows an image decomposed in its bitplanes.

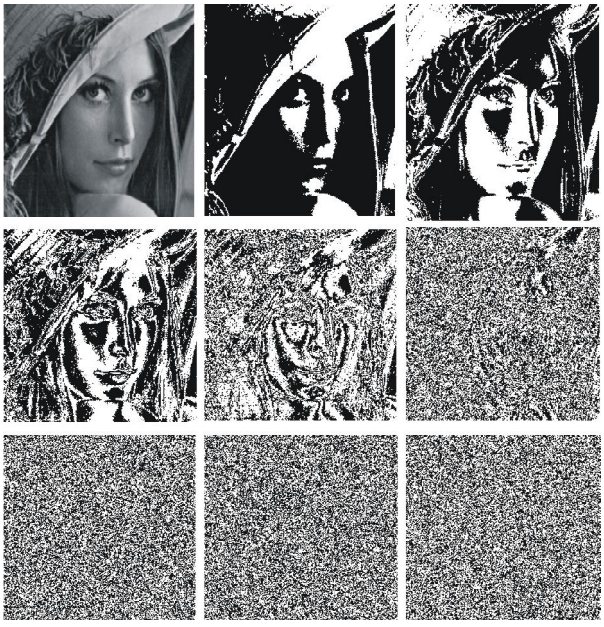

Figure: 2.1 *LENA and her biplanes (i_7, …, i_0) starting from the most significant bit.*

The highest biplanes exhibit some similarities with the gray level image, but the least significant biplanes look random. Because encrypted bits also look random, the encryption of least significant biplanes will add noise to the image [10].

The first "naive" method we have implemented consists in the encryption of the least significant bits as illustrated in Table. In the same table, we provide two distortion measures as well: the *Mean Square Error* (MSE) and the *Peak Signal* to *Noise Ratio* (PSNR). An advantage of the technique that encrypts the least significant bits is that plaintext attacks are harder on random like data [10].

It should be noted that the security is linked to the ability to guess the values of the encrypted data. For example, from a security point of view, it is preferable to encrypt the bits that look the most random. However in practice, the tradeoff is more difficult because the most relevant information, like DC coefficients in a JPEG encoded image, usually are highly predictable [8].

As can be seen from the images drawn in Table 1, we need to encrypt at least 4 to 5 bitplanes before the degradation is visible. In theory the naive method is relatively robust to plaintext attacks because it encrypts bitplanes that contain nearly uncorrelated bit values. Next is the table that illustrates a naive selective encryption method [8].

Figure 2.2: Illustration of a naive selective encryption method.

(a) Original image

(b) bits encrypted
MSE= 10.6, PSNR = 37.9 [dB]

(c) 5 bits encrypted
MSE = 171, PSNR= 25.8[dB]

(d) 7 bits encrypted

MSE = 2704, PSNR=13.8 [dB]

4. DIGITAL WATERMARKING IMPLEMENTED USING JAVA

Since a watermark is merely a sequence of pseudo-random numbers, error free detection may be possible by using linear block codes. With the exception of [11] most watermarking schemes do not employ error-correction. This research work will attempt to implement a new watermarking method using error-correction techniques. Tests will be performed to see if the watermark satisfies the desired properties mentioned in section 2. Furthermore, this research work will determine if the error-correcting watermark scheme will hold any advantages over traditional watermarking methods.

5. METHODOLOGY

In Our Technique We are representing each pixel as a matrix Say name is color matrix A color matrix is a matrix that contains values for channels. It's a 5x5 matrix which represents values for the Red, Green, Blue, Alpha channels and another element w, in that order (R, G, B, A, w). In a Color Matrix object, the diagonal elements of the matrix define the channel values viz. (0, 0), (1, 1), (2, 2), (3, 3), and (4, 4), in the order as specified before –(R G B A w). The values are of type float,

and range from 0 to 1. The element w (at (4, 4)) is always 1.What you have to do is to create a new Color Matrix instance with the desired channel values. As we want to control the alpha blend channel, we should set the element at (3, 3) to the desired value as shown below:

```
ColorMatrix ClrMatrix =
    {
    1.0f, 0.0f, 0.0f, 0.0f, 0.0f,
    0.0f, 1.0f, 0.0f, 0.0f, 0.0f,
    0.0f, 0.0f, 1.0f, 0.0f, 0.0f,
    0.0f, 0.0f, 0.0f, 1.0f, 0.0f,
    0.0f, 0.0f, 0.0f, 0.0f, 1.0f,
    };
```

The **0.5f** value in the above code represents the alpha blend value. 0.5 means semi transparent (50%).

5.1 Quality Metrics

Signal-to-noise (SNR) measures are estimates of the quality of a reconstructed image compared with an original image. The basic idea is to compute a single number that reflects the quality of the reconstructed image. Reconstructed images with higher metrics are judged better. In fact, traditional SNR measures do not equate with human subjective perception. Several research groups are working on perceptual measures, but for now we will use the signal-to-noise measures because they are easier to compute. Just remember that higher measures do not always mean better quality. The actual metric we will compute is the peak signal-to-reconstructed image measure which is called PSNR. Assume we are given a source image f(i,j) that contains N by N pixels and a reconstructed image F(i,j) where F is reconstructed by decoding the encoded version of f(i,j). Error metrics are computed on the luminance signal only so the pixel values f (i,j) range between black (0) and white (255).First you compute the mean squared error (MSE) of the reconstructed image as follows

$$MSE = \frac{\sum \left[f(i, j) - F(i, j) \right]^2}{N^2}$$

The summation is over all pixels. The root mean squared error (RMSE) is the square root of MSE. Some formulations use N rather N^2 in the denominator for MSE.

PSNR in decibels (dB) is computed by using

$$PSNR=20Log_{10}(255 / RMSE)$$

Typical PSNR values range between 20 and 40. They are usually reported to two decimal points (e.g., 25.47). The actual value is not meaningful, but the comparison between two values for different reconstructed images gives one measure of quality.

6. RESULTS & ANALYSIS

6.1 Selective Encryption Method vs. Pixel Correlation Method

The Image Encryption is firstly applied to grey scale images for that case I have taken Lena's image as a test image. Different results have been observed with varying the Alpha by computing the performance measure like MSE, RMSE, and PSNR for an Encrypted/Watermarked Image. The results are then compared with Selective Encryption Method as shown in the table below.

Figure 6.1 Original Lena

Figure 6.2 Selected Watermarks

Table 6.1 Image Encryption Results by using Naive Method

Images	Resolution	Pixel Depth	Alpha	MSE	PSNR (dB)
Lena	512 x 512	24	0.1f	7.50	39.42
Lena	512 x 512	24	0.2f	4.74	41.38
Lena	512 x 512	24	0.3f	3.51	42.68
Lena	512 x 512	24	0.4f	2.76	43.72

Table 6.2 Image Encryption Results by Pixel Correlation Method

Images	Resolution	Pixel Depth	No. of Bits Embedded	MSE	PSNR (dB)
Lena	512 x 512	24	2 Bits	10.6	37.9
Lena	512 x 512	24	3 Bits	171	25.8
Lena	512 x 512	24	5 Bits	2704	13.8
Lena	512 x 512	24	7 Bits	3004	9.8

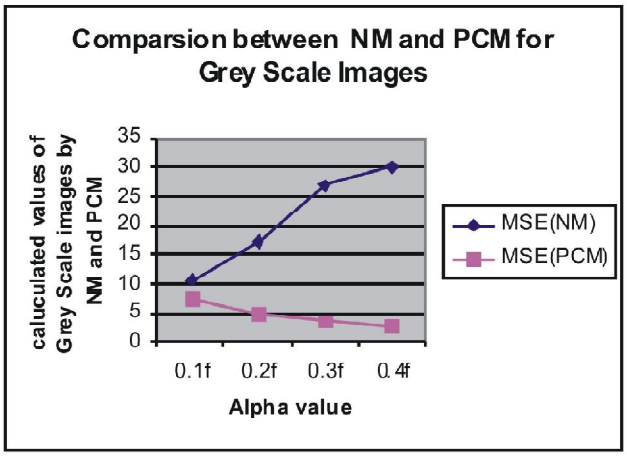

Figure 6.3 Comparison between NM and ACM for Grey scale images

For a single Image we have generated the four graphs as shown. The graph between Alpha & MSE shows that as we increase the value of Alpha Mean Square Error is decreased. We consider Mean square error as a noise in the image, if noise is reduced, then the Quality of watermarked image is improved. The Graph between Alpha & PSNR shows that by increasing the value of alpha PSNR value of an image also increases. If PSNR value is improved then we surely confirmed that image after encryption i.e. watermarked image is of good quality. For example take the encrypted SUNSET image we have Alpha=0.1, MSE=10.04 & PSNR=38.15. Now take another encrypted SUNSET image, we have Alpha=0.2, MSE=6.234 & PSNR=40.19. Hence forth by increasing the value of Alpha, MSE is decreased & PSNR is increased. i.e. Quality of Encrypted image is improved. We have also computed MSE & PSNR with varying Alpha to RGB Components of an image & same results stands true for RGB Component wise analysis.

7. CONCLUSION & FUTURE WORK

This paper represents technique of watermarking making use of human visibility system at different frequencies and gazing effects on different parts of the picture. The watermark generated is semi transparent type i.e. semi visible carrying the advantages of both the visible and the invisible watermark. More over the visibility of watermark is under control of an algorithm and can be very easily changes as per changing requirements. It carries the advantage of the visible watermark i.e. it is

robust and easily visible hence easy to detect the copyright on to the picture. It carries the advantages of non visible watermark also i.e. it does not interfere with the picture elements. It is manually designed by taking care of the picture statistic i.e. value of RGB and W components and more over it is placed on part of the picture which is not so significant portion. The proposed technique is compatible and can be programmed with latest user friendly languages which are in connection with the latest online, E-Commerce and shopping applications as given in the example. More over the proposed method can be applied to all types of image formats e.g. jpeg, bmp etc. Recent work has shown that digital watermarks can be fairly successful in achieving the desired properties mentioned in section 2. These watermarks, however, are not perfect, and more could be done to improve a watermark's robustness or accuracy in detection. Furthermore we can rotate the value of alpha channel to get the desired rate of water mark.

The proposed technique has been applied and implemented in example on a digital image however the work can be extended to the video formats by breaking the video in different number of frames

8. REFERENCES

[1] Mitchell D. Swanson, Mei Kobayashi, And Ahmed H. Tewfik, , IEEE "Multimedia Data-Embedding and Watermarking Technologies" PROCEEDINGS OF THE IEEE, VOL. 86, NO. 6, JUNE 1998.

[2] George Voyatzis and Ioannis Pitas University *of Thessaloniki* "Protecting Digital-Image Copyrights: A Framework" IEEE Computer Graphics and Applications January/February 1999.

[3] Ingemar J. Cox, Matthew L. Miller, And Andrew L. Mckellips "Watermarking As Communications With Side Information" Proceedings of the IEEE, Vol. 87, No. 7, July 1999.

[4] Deepa Kundur "Watermarking with Diversity: Insights and Implications" IEEE Multimedia October-December 2001.

[5] Shoemaker, C., "Hidden bits: A survey of techniques for digital watermarking", Independent study, EER 290, spring 2002.

[6] Jiu-ming Luo hg-qing Yuan Xue-hua "Digital Watermark Technique Based on Speech Signal" International Conference on Computational Electromagnetic and Its Applications Proceedings LV. Spring 2004.

[7] JungHee Seo,HungBog Park "Data Protection of Multimedia Contents Using Scalable Digital Watermarking", Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS '05) 2005 IEEE 608-737,Korea.

[8] IMACS Multi conference on "Computational Engineering in Systems Applications"(CESA), October 4-6, 2006, Beijing, China. *"Technical Challenges for Digital Watermarking"*.

[9] Ming-Shi Wang , Wei-Che *"A majority-voting based watermarking scheme for color image tamper detection and recovery"* Chen National Cheng Kung University, No.1, Ta-Hsueh Road, Tainan, 701 Taiwan 22 January 2007.

[10] Chrysochos E., Fotopoulos V., Skodras A., Xenos M., *"Reversible Image Watermarking Based on Histogram Modificatio*n", 11th Panhellenic Conference on Informatics with international participation (PCI 2007), Vol. B, pp. 93-104, 18-20 May 2007, Patras, Greece.

[11] Ming-Shi Wang , Wei-Che *"A majority-voting based watermarking scheme for color image tamper detection and recovery"* Chen National Cheng Kung University, No.1, Ta-Hsueh Road, Tainan, 701 Taiwan 22 January 2007.

[12] Marc Van Droogenbroeck and Raphaël Benedett, "Techniques for a selective encryption of uncompressed and compressed images" In *ACIVS Advanced Concepts for Intelligent Vision Systems*, Ghent, Belgium, pages 90-97, September 2002.